「GDPR 相關指引文件研析」委託研究計畫

結案報告

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 108 年 11 月

「GDPR 相關指引文件研析」委託研究計畫

結案報告

受委託單位：達文西個資暨高科技法律事務所

研究主持人：葉奇鑫

研究期程：中華民國 108 年 2 月至 108 年 11 月

研究經費：新臺幣 95 萬元

國家發展委員會 委託研究

中華民國 108 年 11 月

中文摘要

在 1995 年的歐盟《個人資料保護指令（Directive 95/46/EC）》施行 21 年後，歐盟於 2016 年 5 月 24 日發布《一般資料保護規則（General Data Protection Regulation, GDPR）》，並於 2018 年 5 月 25 日施行。GDPR 強化個人於數位時代的基本權利，並為公務機關與非公務機關在數位單一市場下的個人資料運用行為提供明確規範，同時消弭不同成員國個人資料保護法律體系間的分歧及不必要的行政負擔。

歐盟在《個人資料保護指令》下設有「第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）」，現於 GDPR 下改設為「歐洲個人資料保護委員會（European Data Protection Board, EDPB）」，職責包含制定發布關於個人資料保護指令及 GDPR 的指引文件，進一步闡釋或舉例說明相關條文之具體適用情形。

鑒於我國刻正辦理向歐盟申請適足性認定事宜，同時考量我國部分公務機關與非公務機關亦可能有 GDPR 之適用，應有必要瞭解相關指引文件之詳細內容，據此，國家發展委員會挑選 11 份指引文件作為研析標的，並將其翻譯為中文供各界參考。

Abstract

After 21 years from *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data(1995)*, EU has published *Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, also known as General Data Protection Regulation (GDPR).

GDPR entered into force on 24 May 2016 and applies since 25 May 2018. The regulation strengthens individuals' fundamental rights in the digital age and clarifies rules for government or non-government agencies in the digital single market. GDPR also do away with the current fragmentation in different national data protection legal systems among member states and unnecessary administrative burdens.

The former Article 29 Data Protection Working Party (WP29) under Directive 95/46/EC has been replaced by European Data Protection Board (EDPB) under GDPR. The mission of WP29 and EDPB includes adopting and publishing guidelines to further interpret Directive 95/46/EC and GDPR by explaining the rules and/or giving examples.

Due to the ongoing process of the government to apply for the adequacy decision from EU Commission and the fact that some of data controllers and processors from Taiwan may be subject to GDPR, it is necessary to comprehend those guidelines. Hence, the National Development Council (NDC) has selected 11 guidelines to translate into Chinese for reference.

目錄

壹、背景說明

歐盟於 1995 年發布個人資料保護指令（Directive 95/46/EC），由各成員國依此指令訂定內國個人資料保護法規與措施。

隨著科技發展的迅速，資料控管者（Controller）對於當事人（Data Subject）個人資料的蒐集、處理與利用的廣度與深度已非 1995 年制定的指令所能涵蓋，且當事人的權利亦隨著資料控管者的強勢而更顯不足，有鑒於此，為消弭資料控管者與當事人間的權責失衡，並對受資料控管者委託的受託運用者（Processer）亦加諸受規管之責，同時就歐盟境內成員國的適用法律與監管方式給予一致性的規範，歐盟遂於 2012 年提出一般資料保護規則（General Data Protection Regulation, 下稱 GDPR）草案，並在 2016 年 5 月公布（第 2016/679 號），取代原有個人資料保護指令，施行日期則為 2018 年 5 月 25 日，於歐盟各成員國內直接生效。

然而，無論個人資料保護指令或 GDPR，法條規範必然有其解釋或適用上的疑義，因此歐盟在個人資料保護指令下設有「第 29 條個資保護工作小組（Article 29 Data Protection Working Party, WP29）」，現於 GDPR 下改設為「歐洲個人資料保護委員會（European Data Protection Board, EDPB）」，職責包含制定發布關於個人資料保護指

令及 GDPR 的指引文件，進一步闡釋或舉例說明相關條文之具體適用情形，以利各成員國受規範的資料控管者及受託運用者遵循。

鑒於我國刻正辦理向歐盟申請適足性認定事宜，同時考量我國部分公務機關與非公務機關亦可能有 GDPR 之適用，均有需要進一步瞭解相關指引文件之詳細內容，據此，國家發展委員會挑選 11 份指引文件作為研析標的並將其翻譯為中文，完成後將公布於國家發展委員會官網之 GDPR 專區，供各界參考。

貳、指引評析

一、同意之指引（WP259 rev.01）

（一） 指引重要內容

本指引於 2017 年 11 月 28 日通過，並於 2018 年 4 月 10 日通過最新修訂版本，旨在對 GDPR 中關於同意的概念提供完整分析。依據 GDPR 第 6 條之規定，同意屬運用個人資料的六個合法基礎之一，但同意有其法定條件必須滿足，此為當事人之同意是否有效之關鍵。

在 GDPR 規範下，有效同意必須具備「自主性」、「特定性」、「（當事人）知情性」、「非模糊性」等要素，且當事人可隨時「撤回同意」，又資料控管者須對取得有效同意負舉證責任。

本指引即對前述各項「有效同意之要素」提出具體說明，並提供示例供各界參考。

（二） 與我國比較

相較之下，我國個人資料保護法未對同意之內涵有具體定義，僅於第 7 條就同意之要件規定蒐集、處理之同意以蒐集者向當事人告知法定事項為前提；目的外利用之同意以蒐集者向當事人告知利用目的、範圍及不同意之影響為前提（兩者性質類似 GDPR 中的知情性），並課予蒐集者對取得同意之事實負舉證責任。

我國個人資料保護法雖未如 GDPR 對前開同意之要素有明確規範，但可從個人資料保護法第 7 條同意之規定，連結第 8 條、第 9 條法定告知事項，推知個人資料保護法就同意仍須具特定性、非模糊性等內涵，以及雖未明文賦予當事人「撤回同意之權利」，但從法理而言，同意係當事人自由表達意願之意思表示，應可隨時撤回同意。

二、GDPR 效力之地域範圍之指引（Guidelines 3/2018）

本指引於 2019 年 11 月 12 日通過，旨在解釋 GDPR 第 3 條關於該法適用之地域範圍的規定。

依 GDPR 第 3 條規定，GDPR 適用於「資料控管者或受託運用者在歐盟境內設立之據點所為之個人資料運用活動，不論該運用是否發生於歐盟境內」，即便未於歐盟境內設立據點，但如資料控管者或受託運用者「對歐盟境內之當事人提供商品或服務，不問是否需要當事人付款」或「對當事人於歐盟境內所為行為進行之監控」時，亦同樣受 GDPR 的拘束。

由此可知，GDPR 之域外效力為該法具有全球影響力的關鍵，但條文所稱據點之判斷、運用個資行為是否發生於歐盟境內之判斷、對歐盟境內當事人提供商品或服務之判斷、監控當事人於歐盟境內之行為的判斷等，均仍有模糊空間。

是本指引即就 GDPR 第 3 條關於地域範圍的規定提出解釋與示例供各界參考。

三、跨境傳輸例外之指引（Guidelines 2/2018）

（一） 指引重要內容

本指引於 2018 年 5 月 25 日通過，旨在就 GDPR 規範下的（個人資料）跨境傳輸限制的例外情形提出說明。

依 GDPR 第 5 章規定，原則上僅在資料接收者所在地經歐盟認定具備個人資料保護法規之適足性時，始可跨境傳輸原儲存於歐盟境內之個人資料，但亦有例外情形可茲適用。

本指引即對 GDPR 第 49 條規定的特殊例外情形提出具體說明，包含：

1、 當事人在被告知由於缺乏適足性認定和適當安全維護措施而導致資料傳輸對當事人可能造成的風險後，明確同意跨境傳輸。

2、 跨境傳輸是對履行當事人與控管者間之契約、或依當事人之請求於執行契約採取特定措施之必要行為。

3、 跨境傳輸對締結或履行控管者與其他自然人或法人間，基於當事人之利益所締結之契約為必要。

4、 基於公共利益之重要原因而有必要跨境傳輸。

5、 為建構、行使或防禦法律上之請求而有必要跨境傳輸。

6、 在當事人身體上或法律上無法為同意之表示時，跨境傳輸對保護當事人或其他人之重大利益為必要。

7、 由公眾登記處所為之跨境傳輸。

8、 跨境傳輸是為控管者的正當利益（需優於當事人之利益）。

（二） 與我國比較

相較於 GDPR「原則禁止」跨境傳輸個人資料之保護機制，我國個人資料保護法第 21 條規範跨境傳輸個人資料，僅在有條文列舉之情形時，始例外禁止非公務機關將個人資料跨境傳輸至境外。

此規範與 GDPR 對於跨境傳輸個人資料之態度存有差異，考量對於我國境內當事人的個人資料之保護程度及我國刻正爭取通過歐盟適足性認定的需求，立法機關似可將我國個人資料保護法對於跨境傳輸個人資料之機制納入評估調整的範圍。

四、個人資料侵害通知之指引（WP250 rev.01）

（一） 指引重要內容

本指引於 2017 年 10 月 3 日通過，並於 2018 年 2 月 6 日通過最新修訂版本，旨在對於 GDPR 中有關事故通知（通報監管機關及通知當事人）之規定提出說明。

GDPR 第 33 條及第 34 條分別課予資料控管者將個人資料侵害事故通報監管機關及通知當事人之義務（但有例外），本指引即進一步

對條文中規定的各項要件（例如通知時點、通知方式、跨境侵害、通知義務的例外等）提供具體說明與示例供各界參考。

（二） 與我國比較

相較之下，我國個人資料保護法第 12 條僅課予公務機關或非公務機關將個人資料侵害通知當事人之義務，未明文要求須將事故通報主管機關，目前實務上多由主管機關於其依個人資料保護法第 27 條第 3 項授權訂定的法規命令中規定非公務機關的通報義務。但由於母法並未明定，而係由主管機關視需求於法規命令規定，後續可再評估是否須於母法統一明確規定，以利個人資料保護更加周延。

又在通知當事人方面，法條未區分情節輕重（例如對當事人造成損害的風險高低、公務機關或非公務機關採取必要措施控管風險的情形)而一律要求公務機關或非公務機關將事故通知當事人(無例外），是否反亦增加當事人不必要之擔憂或困擾，似有評估法規需否調整的空間。

五、個資保護長之指引（WP243 rev.01）

（一） 指引重要內容

本指引於 2016 年 12 月 13 日通過，並於 2017 年 4 月 5 日通過最新修訂版本，旨在闡明 GDPR 於個資治理方面將設置「個資保護長（Data Protection Officer, DPO）」納入法律規範的具體細節。

GDPR 將個資保護長視為個資治理架構下的關鍵參與者，並作為監管機關、當事人及資料控管者或受託運用者間的中介溝通角色，於第 37 條至第 39 條要求公務機關及符合特定條件之非公務機關指派個資保護長，並規範其職位與任務。

本指引即就強制指派個資保護長之條件（以運用個人資料為核心業務，且對當事人為大規模的經常性與系統性監控）、個資保護長之專業能力及技能、個資保護長之獨立性、任務內涵、必要資源等法條規範提出細部說明供各界參考。

（二） 與我國比較

相較之下，我國個人資料保護法並未要求蒐集機關應有個資保護長一職[1]，雖然施行細則第 12 條第 2 項第 1 款說明公務機關或非公務機關的安全措施得包含「配置管理之人員及相當資源」，但對於所稱「管理之人員」的任務內涵、於機關內之地位，以及可享有之資源等無具體規定，在個資治理的強度上與 GDPR 即有落差。

[1] 個人資料保護法第 18 條規定「公務機關保有個人資料檔案者，應指定**專人**辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」，要求公務機關須「指定專人」辦理安全維護事項，但對該專人之「能力」、「任務」、「資源」以及「是否具有獨立性」等則未有規範，與 GDPR 對「個資保護長」的要求仍有落差。

六、透明化之指引（WP260 rev.01）

（一） 指引重要內容

本指引於 2017 年 11 月 29 日通過，並於 2018 年 4 月 11 日通過最新修訂版本，旨在就資料控管者如何滿足 GDPR 中的透明化原則（法定資訊揭露）之措施提出建議。

透明化原則的有效落實取決於資料控管者與當事人的溝通是否足使當事人明確瞭解資料控管者所揭露法定必要資訊的內容，GDPR 第 12 條要求相關資訊必須「簡潔、透明、易懂、便於取得，且須使用清晰的語言文字」，本指引即對上述條件提出說明與示例。

此外，以何種方式向當事人揭露法定必要資訊亦為透明化原則的關鍵，本指引即提出分層聲明、即時彈跳通知、滑鼠游標懸停通知、隱私儀表板、物聯網裝置語音警示等實務應用供各界參考。

（二） 與我國比較

相較之下，我國個人資料保護法第 8 條及第 9 條雖然亦規範蒐集之公務機關或非公務機關向當事人揭露法定必要資訊的告知義務，但一方面未明文要求蒐集之公務機關或非公務機關應使用普遍易懂的方式揭露內容，亦僅於施行細則第 16 條說明告知方式包含言詞、書面、電話、簡訊、電子郵件等足以使當事人知悉或可得知悉之方式，並未就實務操作情形提出建議（於法條中或許亦難以提出建議）。未

來應可考量由各主管機關以行政指導、發布函釋或其他適當方式協助蒐集之公務機關或非公務機關以有效方式滿足告知義務。

七、個資保護影響評估之指引（WP248 rev.01）

（一） 指引重要內容

本指引於 2017 年 4 月 4 日通過，並於 2017 年 10 月 4 日通過最新修訂版本。

個資保護影響評估（Data Protection Impact Assessment, DPIA）作為 GDPR 關於個資治理的一項工具，其目的在於供資料控管者於事前檢視個人資料之運用的必要性、合比例性及潛在風險與因應風險的措施，以此降低事後矯正的法遵成本。

本指引即就如何辦理個資保護影響評估提出遵循步驟建議，並於指引中臚列各國相關評估方法供各界參考。

此外，GDPR 第 35 條規定僅在「可能對自然人之權利和自由造成高風險」的情形，資料控管者始有義務辦理個資保護影響評估（但即便無高度風險，個資保護影響評估亦不失為控管組織風險的措施），因此本指引亦對「是否具有高風險」提出判斷標準，供資料控管者以茲因應。

（二） 與我國比較

相較之下，我國個人資料保護法未將個資保護影響評估納入公務機關或非公務機關的安全維護措施建議事項。雖然施行細則第 12 條第 2 項第 3 款規定「個人資料之風險評估及管理機制」可做為安全維護措施之一，但由於未對此有具體內涵規定，目前實務上仍多以「資訊安全中的風險評鑑」概念作為基礎，即以「資產清查」的角度盤點個人資料（檔案），並予鑑別價值（分級），再依「風險識別」發現的威脅等級與弱點等級，加乘得出個人資料（檔案）之風險值，並針對不同風險值採取對應措施。

此與 GDPR 將資產（靜態個人資料檔案）安全及流程（動態個人資料運用行為）合法性一併作為評估要素的個資保護影響評估仍有落差，應可納入法規調整的評估方向。

八、自動化個人決策與剖析之指引（WP251 rev.01）

（一） 指引重要內容

本指引於 2017 年 10 月 3 日通過，並於 2018 年 2 月 6 日通過最新修訂版本。

由於資料控管者以自動化方式剖析當事人或對當事人作出決策之情形日益增加，此行為或將嚴重影響當事人對其個人資料的自主與控制權，GDPR 即對此風險制定法規以茲因應，並特重當事人之「被

告知權」及「拒絕權」，本指引即在解釋 GDPR 關於自動化個人決策與剖析之規定的具體細節，並提出實務操作建議。

（二） 與我國比較

相較之下，我國個人資料保護法並未明確識別自動化個人決策與剖析之個人資料利用情境，因此並無對此行為訂定細緻規範。考量現今資料分析、人工智慧等技術的快速發展，未來建議參考 GDPR 之規定及本指引之說明，評估是否調整對應法規。

九、資料可攜權之指引（WP242 rev.01）

（一） 指引重要內容

本指引於 2016 年 12 月 13 日通過，並於 2017 年 4 月 5 日通過最新修訂版本，旨在對 GDPR 第 20 條賦予當事人資料可攜之權利內涵提出進一步闡釋。

為強化當事人對其個人資料的控制權並能從中獲益，GDPR 第 20 條第 1 項規定「當事人應有權利以結構性、一般性和機器可讀性之格式接收其提供予控管者與自身相關之個人資料，並有權利將此些資料傳輸至另一資料控管者，而不受其提供個人資料之控管者之妨礙...」，此權利將使當事人除能消極存取資料控管者保有之（其本人的）個人資料外，更能積極利用資料控管者保有的個人資料創造新的價值。

本指引即對此提出細緻說明，解釋資料可攜權的行使前提、行使內容，以及執行方式建議。

（二） 與我國比較

相較之下，我國個人資料保護法第 3 條在類似範圍內賦予當事人有查詢、閱覽個人資料，以及請求製給複製本之權利，並未要求公務機關或非公務機關應滿足當事人資料可攜的權利行使，尚難讓當事人可活用其保存於公務機關或非公務機關之個人資料。

在個人資料開放創新應用的趨勢下（例如金融科技領域下的開放銀行 Open Banking），是否創設當事人的資料可攜權，建議納入評估法規調整的方向。

十、識別主責監管機關之指引（WP244 rev.01）

本指引於 2016 年 12 月 13 日通過，並於 2017 年 4 月 5 日通過最新修訂版本，旨在協助資料控管者或受託運用者於歐盟境內跨（國）境傳輸個人資料時，判斷何國監管機關為其主責監管機關。

由於 GDPR 直接於歐盟各成員國生效，為降低資料控管者或受託運用者的法遵成本，GDPR 採取一站式監管機制，即當資料控管者或受託運用者的個人資料運用行為發生於歐盟境內不同成員國時，將以其中一國的監管機關作為該資料控管者或受託運用者的主責監管機關，並可協調任何涉及其他相關監管機關之執法。

本指引即對如何識別主責監管機關提出判斷標準供資料控管者及受託運用者參考。

十一、 行政罰鍰適用與制定之指引（WP253）

本指引於 2017 年 10 月 3 日通過，旨在向歐盟成員國各監管機關提供適用 GDPR 執行裁罰時判斷行政罰鍰範圍的標準。

由於 GDPR 直接於歐盟各成員國生效，為消弭各成員國監管機關依 GDPR 作出行政罰鍰的基準差異，本指引即提出數項審查依據，期能讓各監管機關有一致性的裁罰基礎，包含：

1、 違反 GDPR 的性質。

2、 涉及當事人之數量及受影響的個人資料的類別。

3、 當事人遭受損害的程度。

4、 違反 GDPR 的持續期間。

5、 主觀上的故意或過失。

6、 為減輕當事人損害所採取的行動。

7、 事前採取的技術性與組織性措施為何，有無遵循何種行為守則或取得何種認證。

8、 先前有無違反 GDPR 的行為。

9、 與監管機關的配合程度。

10、是否主動通報監管機關。

參、指引翻譯

詳如後附。

17/EN
WP259rev.01

Article29 Working Party
第29條個資保護工作小組

Guidelines on consent under Regulation 2016/679
關於第2016/679號規則(GDPR)中的同意之指引

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018
2017年11月28日通過
2018年4月10日最後修訂並通過

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA
關於個人資料運用之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,
having regard to Articles 29 and 30 thereof,
having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，
基於該指令第29條及第30條，
基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:
通過此份指引：

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
網址：http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Contents 目錄

1. Introduction
導言

These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011on consent. The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

本指引對2016/679規則，即一般資料保護規則（以下稱為GDPR）中的同意之概念提供詳盡的分析。在資料保護指令（以下稱為95/46/EC指令）與電子隱私指令中使用迄今的同意之觀念已有所演進。GDPR對於獲得及舉證有效同意之規範，提出進一步的澄清與詳細說明。本指引聚焦於這些變動，提出實務指引以確保GDPR的遵循性，並以15/2011關於同意之意見為基礎。控管者有義務創新找尋新的解決方案以在法律界限內運作，並更佳得維持個人資料與當事人利益之保護。

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.[1] When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing.
如GDPR第6條所列舉[1]，同意仍為運用（譯註：我國個資法將個資之使用分為蒐集(collection)、處理 (processing)、利用 (use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本譯文因此將GDPR中的processing譯為「運用」，而 processor 譯為「受託運用者」）個人資料的六種合法基礎之一。當啟動涉及運用個人資料之行動時，控管者必須花些時間考量何者對該設想的運用是最適當的合法根據。

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[2]
一般來說，同意只有在當事人取得控制權，且對於接受或拒絕條件，或拒絕條件而免受損害享有真正的選擇時，才可作為適當的合法基礎。在尋求同意時，控管者有責任評估是否符合獲得有效同意的所有規範。如完全遵守GDPR而獲得，同意即為賦予當事人對與其有關之個

[1] Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.
GDPR第9條對特種個資的運用禁止提供數項可適用的例外。其中之一即是當事人明確同意使用該資料。

[2] See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.
見15/2011關於同意的定義之意見書（WP187），第6頁至第8頁，及/或06/2014關於95/46/EC指令第7條下的資料控管者之正當利益的概念之意見書（WP217），第9頁、第10頁、第13頁及第14頁。

人資料可否被運用之控制權的工具。若否，則當事人的控制權形同虛設，而同意將成為無效的運用依據，並導致運用行為違法[2]。

The existing Article 29 Working Party (WP29) Opinions on consent[3] remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.
現有的第29條工作小組（WP29）關於同意的意見[3]仍然具有相關性，這與新的法律框架一致，因為GDPR納入了現有的WP29指引和一般優良實務，並且GDPR下的大多數有關同意的關鍵要素保持不變。因此，在本文件中，WP29擴充並完備了早期關於特定主題的意見，其中也包括95/46/EC指令下的同意，而不是替換它們。

As stated in Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.[4] The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.[5]
正如意見15/2011中關於同意的定義所述，要求他人接受的資料運用作業應該受到嚴格規範，因為它涉及當事人的基本權利，並且若未經當事人同意，控管者對資料的運用作業即為非法[4]。「歐盟基本權利憲章」第7條和第8條強調了同意的重要性。此外，獲得同意並非否定或以任何方式限縮控管者遵守GDPR中有關資料運用原則的義務，尤其是GDPR第5條關於公平性、必要性、比例性以及資料品質的義務。即便運用個資是基於當事人的同意，但與特定資料運用目的無必要的資料蒐集，既不合法，基本上也不公平[5]。

Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.[6] Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.[7]
同時，WP29也意識到對電子隱私指令（2002/58/EC）的審查。電子隱私規則草案中的同意

[3] Most notably, Opinion 15/2011 on the definition of consent (WP 187).
尤其是15/2011關於同意的定義之意見書（WP187）。
[4] Opinion 15/2011, page on the definition of consent (WP 187), p.8
15/2011關於同意的定義之意見書（WP187），第8頁。
[5] See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.
見15/2011關於同意的定義之意見書（WP187），以及GDPR第5條。
[6] According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.
依電子隱私規則草案第9條規定，該規則適用GDPR第4條第11款及第7條關於同意的定義與要件。
[7] See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).
見03/2016關於電子隱私指令的評估與審查之意見書（WP240）。

之概念仍準用GDPR中的同意之概念[6]。組織在電子隱私法規下，對於大部分的線上行銷訊息或行銷電話，以及包含使用cookies或行動應用程式或其他軟體在內的線上追蹤手段，可能都需要獲得同意。WP29已向歐洲立法機關就電子隱私規則之草案提出建議與指引[7]。

With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.[8] This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. WP29 notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.
對於現有的電子隱私指令，WP29指出原本應參照已廢止的95/46/EC指令之處，應解釋為參照GDPR[8]。此亦適用於現行2002/58/EC指令中的同意之參照，因為電子隱私規則在2018年5月25日時（尚）不會生效。依GDPR第95條規定，在電子隱私指令就「以大眾通訊網路提供大眾電子通訊服務」所涉及的運用已課予特定義務之範圍內，GDPR即不再對相同目標課以額外義務。WP29指出，GDPR下的同意之規範並不構成「額外義務」，反而是合法運用的先決條件。因此，GDPR關於獲得有效同意之條件，對於落入電子隱私指令範圍之情形即有適用。

2. Consent in Article 4(11) of the GDPR
GDPR第4條第11款規定之同意

Article 4(11) of the GDPR defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*
GDPR第4條第11款將同意定義為：「*當事人為表達同意運用與其有關之個人資料，藉由聲明或清楚肯定之行動而自由給予之特定、知情及非模糊之意思表示*」。

The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.[9] Besides the amended definition in Article 4(11), the GDPR provides additional

[8] See Article 94 GDPR.
見GDPR第94條。

[9] Consent was defined in Directive 95/46/EC as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" which must be 'unambiguously given' in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.
95/46/EC指令對同意的定義為「當事人為表達同意運用與其有關之個人資料所自由給予之特定且知情的意思表示」，且須「非模糊地給予」才可使該個資運用行為合法（95/46/EC指令第7條第a項）。見15/2011關於同意的定義之意見書（WP187）中有關以同意作為合法基礎的適當性的範例。在該意見書中，WP29對於如何區別「以同意作為適當的合法基礎」以及「以充足正當利益作為合法基礎（或許伴隨選擇退出的機會）」或「建議採用契約關係作為合法基礎」提出指引。見第29條工作組06/2014意見書，第14頁，第III.1.2段以下。明確同意同時也是禁止運用特種個資的一項例外：見GDPR第9條。

guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.
同意的基本觀念仍與95/46/EC指令中基本觀念的相似，且依GDPR第6條規定[9]，同意是個人資料運用所須依據的合法基礎之一。除了第4條第11款修正的定義之外，GDPR於第7條及前言第32點、第33點、第42點與第43點，就控管者須如何行動以遵循同意之規範的重要要素提出額外指引。

Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.
最後，條文中包含撤回同意的具體條款及前言，即確認同意應為可逆的決定，當事人一方仍有一定程度的控制權。

3. Elements of valid consent
有效同意的要素

Article 4(11) of the GDPR stipulates that consent of the data subject means any:
GDPR第4條第11款規定當事人的同意係指任何：

- freely given,
  自主給予
- specific,
  特定
- informed and
  知情以及
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
  非模糊的當事人意思表示，即藉由聲明或清楚肯定之行動，表達同意運用與其有關之個人資料。

In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR. [10]以下章節將分析第4條第11款規範控管者改變其同意之要求／形式的文義範圍，以確保GDPR的遵循性[10]。

3.1. Free / freely given[11]

[10] For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.
關於依據95/46/EC指令的同意規範而進行的運用活動，其指引詳見本文件第7章及GDPR前言第171點。

[11] In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).
WP29在幾份意見書中探討在無法自主給予同意的情形將使同意受到的限制。特別是15/2011關於同意的定義之意見書（WP187）、關於運用與電子健康紀錄有關健康資訊的個人資料之工作文件（WP131）、8/2001關於雇傭關係中的個人資料運用之意見書（WP48），以及4/2009關於世界運動禁藥管制組織（WADA）隱私與個人資訊保護國際標準、世界運動禁藥管制規範相關條文，以及WADA與（國家）反禁藥組織對抗運動禁藥中的隱私議題所涉個資運用行為之第二份意見書（WP162）。

自主性/自主給予[11]

The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[12] If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.[13] The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

「自主」要素意指當事人真正的選擇與控制權。作為一部通用規則，GDPR規定若當事人未能獲得真正的選擇，或受到強迫而作出同意，或如不同意將使其遭受負面後果時，該同意即為無效[12]。如將同意綑綁於條款與條件中，成為無法磋商的一部分時，即推定為非自主給予。因此，若當事人無法拒絕或撤回同意而免受任何損害時，其同意即不被認為具備自主性[13]。GDPR亦將控管者與當事人間的不對等之概念納入考量。

When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words "inter alia", meaning that there may be a range of other situations which are caught by this provision. In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

在評估同意是否自主給予時，也應考量第7條第4項所描述將同意與契約或提供之服務綑綁的情形。第7條第4項使用「特別是」(inter alia)一詞以例示方式草擬該條款，即表示得有其他情形落入本條款規範。大體而言，任何對當事人造成不適當之壓力或影響而使當事人無法行使自由意願的要素（可能以許多不同方式顯現），均應導致同意無效。

> [Example 1]
> A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.
>
> [示例1]
> 某相片編輯行動應用程式向使用者要求啟用衛星定位功能以使用其服務。此應用程式亦告知使用者將基於行為廣告之目的而利用所蒐集的資料。無論地理位置或線上行為廣告皆非相片編輯服務所必要，且逾越提供其核心服務之範圍。鑒於使用者若不同意該目的即無法使用此應用程式，其同意即無法認定為自主給予。

3.1.1. Imbalance of power
權力不對等

Recital 43[14] clearly indicates that it is unlikely that **public authorities** can rely on consent for

[12] See Opinion 15/2011 on the definition of consent (WP187), p. 12
見15/2011關於同意的定義之意見書（WP187），第12頁。

[13] See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.
見GDPR前言第42點、第43點及WP29於2011年7月13日通過的15/2011關於同意的定義之意見書（WP187），第12頁。

[14] Recital 43 GDPR states: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular

processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.[15]

前言第43點[14]清楚指出，**公務機關**不太可能以同意作為運用個資的依據，因為當公務機關作為一個控管者時，其與當事人之間經常有明顯的權力不對等情形。在大部分案例也明顯存在當事人對於是否接受控管者運用個資（的條件）並無真正的選擇權利之情況。WP29認為，在原則上，應有其他合法基礎更適合作為公務機關行為之依據[15]。

Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

在不牴觸上述總體考量的前提下，GDPR的法律框架並不完全排除公務機關以同意作為運用個資的合法基礎。下列示例即說明某些可適當使用同意的情形。

> [Example 2] A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.
>
> [示例2]某地方政府正在規劃道路養護工程。由於該道路工程可能長時間妨礙交通，該政府提供其市民以電子郵件訂閱工程進度及預期延工等資訊的機會。該政府清楚告知市民並無參與義務，並基於該（單一）目的徵求使用電子郵件地址之同意。不同意的市民不會因此無法獲得該政府的核心服務或無法行使任何權利，因此市民得自主地對該利用行為表示同意或拒絕。該道路工程的所有資訊亦皆可於政府網站上取得。

> [Example 3] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.
>
> [示例3]某自然人擁有之土地需取得地方政府及該地方政府所在地之省政府的特定許可。兩公務機關為發布許可，需取得相同之資訊，但卻無法存取彼此的資料庫。因此，雙方皆要求提供相同之資訊，而該土地所有人即將資料寄送予兩公務機關。地方政府及省政府向該人徵求合併檔案的同意，以避免重複程序及通信聯繫等問題。兩公務機關均保證該同意具選擇性，且若該人不同意合併資料，其許可程序仍將分別進行。該土地所有人即可自主地向公務機關就合併檔案之目的給予同意。

---

where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (…)"

GDPR前言第43點：「為確保同意為自主給予，在當事人與控管者間明顯存有不平等的特定情形，同意無法作為運用個人資料的有效法律基礎，尤其當控管者為公務機關時，在任何情況下都不太可能自主給予同意…」。

[15] See Article 6 GDPR, notably paragraphs (1c) and (1e).

見GDPR第6條，特別是第1項第c款與第1項第e款。

[Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.[16]

[示例4]某公立學校徵求學生同意學校使用其照片以出版學生雜誌。只要學生不會遭拒絕提供教育或服務，並可拒絕學校使用照片而不會受到任何損害，則同意在此情形即具備真正的選擇性[16]。

An imbalance of power also occurs in the **employment** context.[17] Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.[18] Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[19]
權力不對等的情形亦存在於**僱傭關係**中[17]。鑒於雇主與受雇人之間的從屬性，當事人不太可能可拒絕同意雇主運用其個人資料，而毋庸面臨因拒絕所致不利影響的恐懼或實際風險。舉例來說，當雇主要求同意在工作場所啟用例如攝影監視等監控機制，或要求填寫評估表格時，受雇人不太可能可自由回覆同意與否而不感到壓力[18]。因此，WP29認為雇主以同意作為運用現在或未來受雇人個資的依據仍有疑慮，因為同意不太可能是自主給予。基於雇主與受雇人間的關係，對於大部分這種運用與工作相關的個資之情形，其合法基礎不可也不應是受雇人的同意（第6條第1項第a款）[19]。

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[20]
然而這並不代表雇主永遠不可以同意作為運用行為的合法基礎。在某些情況，雇主可能得證明同意為自主給予。鑒於雇主與其員工間的權力不對等，受雇人僅在例外情形，即無論同意與否均不會產生不利結果時，才能夠自主給予同意[20]。

[Example 5]

[16] For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.
為本示例之目的，公立學校係指公家資助的學校或任何具有國家法律認定之公務機關或團體資格的教育機構。

[17] See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created. See also Recital 155.
見GDPR第88條強調的保護受雇人特定利益之需求，以及成員國法律可創造的例外。亦見前言第155點。

[18] See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.
見15/2011關於同意的定義之意見書（WP187），第12頁至第14頁、8/2001關於僱傭關係中的個人資料運用之意見書（WP48）第10章、關於工作場所的電子通訊監控之工作文件（WP55），第4.2段，以及2/2017關於職業環境的資料運用（WP249），第6.2段。

[19] See Opinion 2/2017 on data processing at work, page 6-7
見2/2017關於職業環境的資料運用，第6頁至第7頁。

[20] See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.
見2/2017關於職業環境的資料運用（WP249），第6.2段。

A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

[示例5]

某攝影團隊將拍攝辦公室的特定區域。由於受雇人可能出現於影片的背景中，雇主即向坐在該區域內的受雇人徵求被拍攝的同意。不同意被拍攝者不會以任何方式受到處罰，而僅需在拍攝期間移至該建築內其他區域相同的辦公桌。

Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

權力不對等不僅限於公務機關及僱傭關係，也可能存在於其他情形。如同WP29在數個意見中強調，只有在當事人可行使真正的選擇權，且若不同意亦不會有受欺瞞、脅迫、強制或重大負面結果（例如大量的額外成本）之風險時，其同意方屬有效。當存有任何強迫、壓力或無法行使自由意願的情形時，其同意絕非自主。

3.1.2. Conditionality
條件性

To assess whether consent is freely given, Article 7(4) GDPR plays an important role.[21]

Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.

GDPR第7條第4項對於評估同意是否自主給予扮演重要角色[21]。

GDPR第7條第4項指出，特別是將同意與接受條款或條件「綑綁」，或當運用個人資料並非某契約或服務所必要，卻將提供契約或服務與徵求運用個資之同意「綑綁」一起的情形，都是高度不樂見的。如果同意是在此情形下給予，則將被視為非自主提供（前言第43點）。第

[21] Article 7(4) GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." See also Recital 43 GDPR, that states: "[…] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance."

GDPR第7條第4項：「當評估同意是否自主給予時，應特別在最大程度考量包含提供服務在內的契約履行是否以同意運用履行契約非必要的個人資料為條件」。亦見GDPR前言第43點：「[…]即便在個案中尚屬適當，若不允許就不同的個人資料運用行為分別給予同意，或儘管同意對履行契約並非必要，卻使包含提供服務在內的契約履行依附於同意時，該同意將推定為非自主給予」。

7條第4項旨在確保當個人資料並非必要時，運用個資之目的不致被提供契約或服務所掩飾或與其綑綁。為了達到此目的，GDPR確保同意運用個資不可成為契約直接或間接之履行對價。同意與契約為合法運用個資的兩種合法基礎，彼此不可合併或模糊界線。

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.
超過嚴格必要範圍而強迫同意使用個人資料，將限制當事人的選擇權，並妨礙其自主同意。由於個資保護法律之目標即在保護基本權利，因此個人對其個人資料的控制極為重要，而對於非必要個人資料之運用的同意，將強烈推定不可視為換得契約履行或服務提供的對價義務。

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.
因此，當控管者將徵求同意與履行契約綑綁一起時，不願意由控管者運用其個人資料之當事人即面臨遭拒絕提供其所求之服務的風險。

To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be necessary for the performance of that contract. According to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.[22] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.
在評估是否有此類綑綁的情形時，重要的是確定該契約的範圍，以及為履行該契約所必要之個人資料。依WP29意見06/2014所述，「履行契約所必要」一語須嚴格解釋。該運用行為必須是完成個別當事人之契約所必要。例如可包含運用當事人的地址以供寄送線上購買之商品，或運用信用卡資訊以完成付款。在僱傭關係的情形，此依據可允許例如運用薪資資訊及銀行帳戶細節以支付薪酬[22]。運用資料與執行契約之目的間，必須具有直接且客觀的連結。

If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.[23]
如控管者有意運用事實上係為履行契約所必要的個人資料，則同意即非適當的合法依據[23]。

Article 7(4) is only relevant where the requested data are **not** necessary for the performance of the

[22] For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).
更多資訊與示例見WP29於2014年4月9日通過之06/2014關於95/46/EC指令第7條下的資料控管者之正當利益的概念之意見書，第16頁至第17頁（WP217）。

[23] The appropriate lawful basis could then be Article 6(1)(b) (contract).
適當的合法基礎可為第6條第1項第b款（契約）。

contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent. Conversely, if processing **is** necessary to perform the contract (including to provide a service), then Article 7(4) does not apply.
第7條第4項僅與「要求非履行契約（包含提供服務）所必要之資料，且根據同意而獲得這些資料是履行契約的條件」相關。相反地，如運用行為是履行契約（包含提供服務）所必要，則第7條第4項即不適用。

[Example 6]
A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.
[示例6]
某銀行要求客戶同意允許第三方基於行銷之目的使用其付款資訊。此運用行為對於履行與客戶間的契約及提供一般性的銀行帳戶服務並非必要。若客戶不同意該運用目的，將導致遭拒絕提供銀行服務、關閉銀行帳戶，或依案例情形增加費用時，該同意即非自主給予。

The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.
立法者選擇在各個推定同意不具自主性的要素中強調條件性，即表示如有條件的存在，則必須詳加檢視。第7條第4項中的「在最大範圍內考量」一語，即指當某契約（包含服務的提供）與要求同意運用個資綑綁一起時，控管者需特別留意。

As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.
由於第7條第4項的文義並非絕對，因此條件性在某些案例仍可能存有極有限的空間，不致使同意不生效力。然而，前言第43點的「推定」一詞清楚指出該類案例屬於高度例外。

In any event, the burden of proof in Article 7(4) is on the controller.[24] This specific rule reflects the general principle of accountability which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.[25]
無論如何，控管者應就第7條第4項負舉證責任[24]。此特別規範反映了貫穿GDPR的課責性一

[24] See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.
見GDPR第7條第1項，控管者須證明當事人的同意為自主給予。

[25] To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.
某程度上，本段是現存WP29指引之彙整。如同在15/2011意見書所述，在當事人基於彼此關係的性質或特殊情況而從屬於資料控管者時，在該背景下（例如僱傭關係或由公務機關蒐集資料），可強力推定該同意之自主性受到限制。在第7條第4項的效力下，控管者較難證明同意是由當事人自主給予。見：15/2011關於同意的定義之意見書（WP187），第12頁至第17頁。

般原則。然而，當第7條第4項適用時，控管者將較難證明同意係由當事人自主給予[25]。

The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.
控管者得主張當事人可在「同意額外目的使用個人資料之服務」與「相同控管者所提供之等同服務，但不需同意額外目的使用個人資料」之中作出選擇，因此其組織已提供當事人真正的選擇權。只要存在使控管者履行契約或提供契約約定的服務，而不需同意其他或額外的資料使用之可能性時，即表示此處不存在有條件的服務。然而，此二種服務必須真正的實質相同。

The WP29 considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand. In such a case, the freedom of choice would be made dependent on what other market players do and whether an individual data subject would find the other controller's services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means this consent fails to comply with the GDPR.
WP29認為，若控管者主張選擇權存在於「由該控管者提供，但須同意額外目的使用個人資料之服務」與「其他控管者提供之等同服務」之間，則該同意不可被認定為自主給予。在此情形中，選擇的自由性將依附於其他市場參與者的行為，以及個別當事人是否認為其他控管者的服務真正等同。且由於競爭者可能事後調整其服務，這表示控管者有義務監看市場發展以確保對其個資運用行為之同意持續有效。因此，提出此主張即表示該同意不符合GDPR的規範。

3.1.3. Granularity
區別性

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.
某項服務可能包含不只一種目的之數個運用行為。在此情形，當事人應可自由選擇接受何種目的，而無須一次同意所有目的。依GDPR規定，在具體個案中，開始提供一項服務前可能需要數個同意。

Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being

appropriate in the individual case. Recital 32 states "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*".
前言第43點清楚指出，若獲得同意的過程/程序並不允許當事人就個別運用個資行為分別給予同意（例如只同意某些運用行為，不包含其他），儘管在個案中尚屬適當，該同意仍將推定為非自主給予。前言第32點表明「*同意應涵蓋所有基於一個或數個目的之運用行為。當運用行為具有數種目的時，應針對所有的目的都需給予同意*」。

If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.
若控管者將運用行為的數種目的合併，又未就各個目的徵求個別同意時，即缺乏自主性。此區別性與下方第3.2段所述之同意明確性的需求具有緊密關聯。當為追求數種目的而運用個資時，區別性便是符合有效同意條件的解決方案，即數種目的之區分，以及針對個別目的獲得同意。

[Example 7]
Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).

[示例7]
某零售商以同一請求，徵求消費者同意使用其個資於寄送行銷電子郵件，並與集團內其他公司分享消費者資訊。由於無法針對這兩個目的個別表示同意，此同意即不具備區別性，因此不生效力。在本案例中，如要將聯絡資訊寄送予商業夥伴，即應蒐集明確的同意。只有在蒐集當事人之同意時已提供個別夥伴的身分，且係基於相同目的（在本例中：行銷目的）而寄送資訊，則此明確同意對個別夥伴而言才被視為具有效力（並參第3.3.1段）。

3.1.4. Detriment
損害

The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.
控管者必須證明，拒絕或撤回同意不會導致任何損害（前言第42點）。舉例來說，控管者須證明撤回同意不會對當事人產生任何花費，從而同意之撤回不存有顯著的不利益。

Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.
其他當事人不予同意而生損害的例子為欺瞞、脅迫、強制或重大負面結果。控管者須能證明當事人對於是否同意享有自主性或真正的選擇權，且可撤回同意而免於任何損害。

If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances.

如控管者可證明對某服務得撤回同意而免於任何負面結果時，例如使用者獲得之服務效能不因此而降級，便可能用以證明該同意為自主給予。GDPR並不排除所有獎勵誘因，但控管者有義務證明在任何情況下，同意仍為自主給予。

[Example 8]

When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).

[示例8]

下載某生活時尚行動應用程式時，該應用程式要求同意存取手機的加速度計。此非執行應用程式所必要，但有助於控管者更瞭解使用者的移動軌跡和活動程度。當使用者日後撤回該同意時，發現該應用程式僅可在有限範圍內運行。這即是前言第42點所稱損害的適例，表示獲得的同意自始即屬無效（從而，控管者必須將所有以此方式蒐集而跟使用者移動軌跡有關之個人資料刪除）。

[Example 9]

A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.

[示例9]

某當事人向時尚產品零售商訂閱一般折扣的產品新訊。該零售商徵求當事人同意蒐集更多購物偏好資料，以便根據其購物歷史或自願填寫的問卷而向其提供符合偏好的產品。當該當事人日後撤回同意時，將再收到非個人化的時尚產品折扣。由於僅損失控管者提供的獎勵誘因，此將不構成損害。

[Example: 10]

A fashion magazine offers readers access to buy new make-up products before the official launch.

The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.

The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.

In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.

[示例10]

某時尚雜誌提供其讀者在產品正式發表前即可購買化妝新品。

該產品隨後即將上市，但此雜誌的讀者可獨家預覽這些產品。為了享受這項優惠，人們必須提供郵寄地址，並同意列於該雜誌的訂閱者郵寄清單。郵寄地址是為寄送所必要，而郵寄清單是用來每年寄送例如化妝品或短衫等產品的商業資訊。

該公司解釋，郵寄清單上的資料將僅用於寄送產品以及該雜誌自己的紙本廣告，且不會與任何其他組

織分享。
鑒於讀者最終仍可購買該產品，因此如讀者不願基於此原因揭露地址，將不致受到任何損害。

3.2. Specific
特定性

Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.[26] The requirement that consent must be '*specific'* aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent.[27] In sum, to comply with the element of 'specific' the controller must apply:

(i) Purpose specification as a safeguard against function creep,
(ii) Granularity in consent requests, and
(iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

第6條第1項第a款確認當事人的同意必須針對「一個或數個特定的」目的而給予，且當事人對個別目的均有選擇權[26]。同意必須「特定」的規範，是為確保當事人擁有一定程度的使用者控制權及透明度。GDPR並未變更此要求，仍密切與「知情」同意的規範連結。同時，解釋上須符合取得「自主」同意的「區別性」要求[27]。簡言之，控管者必須遵守下列條件以符合「特定」的要素：

(i) 目的特定性作為避免用途悄悄擴散的保障，
(ii) 要求之同意須有區別性，以及
(iii) 清楚區分要求同意個資運用行為的資訊與其他事項的資訊。

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.[28] The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

補充 (i)：依GDPR第5條第1項第b款規定，獲得有效同意係以針對有意運用之行為確定其特定、清楚且正當之目的為前提[28]。在當事人同意對於資料的原始蒐集行為後，第5條第1項第b款結合特定同意的要求及目的限制之概念，以此作為避免資料運用之目的逐漸擴大或模糊的保障。此現象亦稱為用途悄悄擴散，由於可能導致控管者或第三人在預期之外使用個資或使

[26] Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).
關於確定「目的」的進一步指引可見於3/2013關於目的限制之意見書（WP203）。

[27] Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.
GDPR前言第43點謂無論適當與否，都必須能對不同的運用行為分別同意。應向當事人提供可分別同意各個目的之區別同意的選項。

[28] See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'."
見WP293/2013關於目的限制之意見書（WP203），第16頁，：「基於這些理由，一個模糊或概括的目的，例如沒有其他細節的『優化使用者體驗』、『行銷目的』、『資訊安全目的』或『將來之研究』等，通常無法符合『特定』的標準」。

當事人失去控制權，對當事人將構成風險。

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.[29] In line with the concept of *purpose limitation*, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.
如控管者依循第6條第1項第a款，則當事人須針對特定的運用目的給予同意[29]。根據第5條第1項第b款及前言第32點的*目的限制*觀念，只要這些行為均基於相同目的，同意之標的可以涵蓋不同行為。顯而易見的是，只有在當事人明確知悉使用其個資之預期目的時，才可獲得特定同意。

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis which better reflects the situation.
儘管對於目的間的相容性設有規範，同意仍須針對特定目的而為。當事人僅在瞭解自己享有控制權，且其個資僅會基於那些特定目的而被運用時，才會給予其同意。在控管者基於同意而運用個資，但又要為其他目的而運用該個資時亦然，即控管者必須就其他的目的另行徵求同意，除非該情形有其他合法基礎可茲適用。

> [Example 11] A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed.
> [示例11]某有線電視網基於訂戶同意而蒐集訂戶的個人資料，依訂戶的收視習慣針對新上架電影向訂戶提出個人化建議。一段時間後，該電視網決定要讓第三方按訂戶的收視習慣寄送（或播送）精準廣告。為了這個新目的，必須獲得新的同意。

Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.
補充(ii)：同意機制不僅須有區別性以符合「自主」的規範，也須符合「特定」之要素。此表示為不同目的徵求同意的控管者，應就各個目的提供個別的「選擇加入」選項，以供使用者就特定目的給予特定同意。

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

[29] This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.
此與15/2011關於同意的定義之意見書（WP187）相符，例如第17頁。

補充(iii)：最後，為讓當事人知悉不同選擇將造成的影響，控管者應就所徵求個別同意以運用個資之各個目的，分別提供特定資訊。如此，當事人方能給予特定同意。本議題與接下來3.3所要討論的控管者應提供清楚資訊之規範有所重疊。

3.3. Informed
知情性

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

GDPR強化知情同意的規範。依GDPR第5條規定，透明化的要求是基本原則之一，且與公平性及合法性原則密切相關。為了讓當事人得在知情前提下作出決定，瞭解自己同意的內容，並行使例如撤回同意的權利，在獲得其同意前事先提供資訊極為重要。若控管者未提供可取得的資訊，使用者控制權即形同虛設，而同意便成為無效的運用個資依據。

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

未符合知情同意規範的結果將導致同意不生效力，而控管者將可能違反GDPR第6條之規定。

3.3.1. Minimum content requirements for consent to be 'informed'
知情同意之內容的最低要求

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

(i) the controller's identity,[30]

(ii) the purpose of each of the processing operations for which consent is sought,[31]

(iii) what (type of) data will be collected and used,[32]

(iv) the existence of the right to withdraw consent,[33]

(v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)[34] where relevant, and

(vi) on the possible risks of data transfers due to absence of an adequacy decision and of

[30] See also Recital 42 GDPR: "[…]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[…]." 30見GDPR前言第42點：「[…]要使同意為知情，當事人應至少知悉控管者的身分及所欲運用個人資料行為之目的[…]」。

[31] Again, see Recital 42 GDPR
同樣見GDPR前言第42點

[32] See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20
見WP29意見15/2011關於同意的定義（WP187），第19頁至第20頁

[33] See Article 7(3) GDPR
見GDPR第7條第3項

[34] See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.
見WP29關於為2016/679號規則之目的的自動化個別決策與建檔指引（WP251），第IV.B段，第20頁以下。

appropriate safeguards as described in Article46.[35]

為使同意具備知情性，必須將某些對作出決定至為重要的要素告知當事人。因此，WP29認為，至少應將下列資訊作為告知內容，以獲得有效同意：

(i) 控管者的身分[30]，

(ii) 徵求同意的各個運用行為之目的[31]，

(iii) 蒐集與利用之個資（類別）為何[32]，

(iv) 有權撤回同意[33]，

(v) 涉及第22條第2項第c款規定[34]時提供關於利用個資以作出自動化決策的資訊，以及

(vi) 依第46條所述[35]，告知因未取得適足性決定且未有適當安全維護措施而傳輸個資的潛在風險。

With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

WP29就上述項目(i)及(iii)提到，在由多數（聯合）控管者徵求同意的案例中，或個資將傳輸予其他控管者或由其他控管者運用，而這些控管者均以原始同意作為法律依據的情形，這些組織的名稱都應揭露。雖然依GDPR第13條及第14條規定，控管者必須提供包含受託運用者在內的個資接受者完整名單或接受者類別，但同意的規範並不要求事先揭露受託運用者之名稱。總之，WP29表示，依個案情形與背景不同，可能須要提供更多的資訊，以便讓當事人真正瞭解即將發生的運用行為。

3.3.2. How to provide information
提供資訊的方式

The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital32. This leads to a higher standard for the clarity and accessibility of the information.

GDPR並未就滿足知情同意之規範而對提供資訊的格式或形式有所規定。這表示得以不同方式呈現有效的資訊，例如書面或言詞聲明，或聲音或影像訊息。然而，GDPR對知情同意訂有數項規範，主要規定於第7條第2項及前言第32點，為資訊的清晰性與可得性設下更高的標準。

When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements

[35] Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19
依第49條第1項第a款規定，在尋求明確同意時，須提供關於不具備第46條所述的安全維護之特定資訊。見WP29意見15/2011關於同意的定義（WP187），第19頁

full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.[36]
在徵求同意時，控管者應確保在任何情況均使用清楚且簡白的語言。這代表該訊息不僅對律師，對一般人來說，也應可輕易理解。控管者不可採用冗長而難以理解的隱私權政策或充滿法律用語的聲明。同意必須清晰且可與其他事項有所區隔，並以可理解且可輕易取得的方式提供。此規範實質上表示，不可將與同意與否的知情決定有關之資訊隱藏於一般的條款與條件中[36]。

A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.[37]
控管者必須確保同意是以「能讓當事人輕易識別控管者身分，並瞭解其所同意的內容為何之資訊」為基礎而提供。控管者須就所尋求同意之個資運用行為清楚描述其目的[37]。

Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.
WP29曾發布關於透明化的指引，對可得性提出其他具體指引。如以電子方式給予同意時，其請求必須清楚而簡潔。階層式及區別性資訊可作為因應「準確且完整」及「可理解性」此雙重義務的適當作法。

A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.[38] After identifying their audience, controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.
控管者必須評估向其組織提供個人資料之受眾種類。例如，目標受眾包含尚未成年之當事人，則控管者應確保未成年人亦可瞭解其資訊[38]。在識別受眾後，控管者必須決定要提供何種資訊，再決定如何向當事人提出該資訊。

Article 7(2) addresses pre-formulated written declarations of consent which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a

[36] The declaration of consent must be named as such. Drafting, such as "I know that…" does not meet the requirement of clear language.
同意的聲明必須表示其為同意。以例如「我知悉…」為文並不符合清楚的語言之規範。

[37] See Articles 4(11) and 7(2) GDPR.
見GDPR第4條第11款及第7條第2項。

[38] See also Recital 58 regarding information understandable for children.
見前言第58點有關兒童可理解之資訊。

paragraph within terms and conditions, pursuant to Recital 32.[39] To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.
第7條第2項提出的定型化書面同意聲明也涉及其他議題。當同意的請求是（書面）契約的一部分時，該請求應清楚與其他事項區別。如書面契約包含與同意使用個人資料無關的許多面向時，對於同意事項應清楚突顯，或呈現於另一份文件。同樣的，如經由電子方式徵求同意，該同意之請求應分列並有所區別，依前言第32點規定[39]，不可僅作為條款與條件的一個段落。考慮到小螢幕或僅在有限空間揭露資訊的情形，可於適當時機，考慮採用階層方式呈現資訊，以避免對使用者體驗或產品設計造成過度干擾。

A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid "informed" consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.
為符合GDPR要求，以當事人同意作為法律依據的控管者，也應因應第13條和第14條規定的個別資訊揭露之義務。實務上，許多案例可能以整合方式，同時遵守資訊揭露義務及知情同意規範。然而，本段是以「即便獲得同意的過程未揭露所有第13條與/或第14條中的要素（但這些要素務必應在其他地方提出，例如公司的隱私聲明），但有效的『知情』同意仍可存在」為理解前提。WP29已就透明化的要求發布另一份指引。

> [Example 12]
> Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.
> [示例12]
> X公司為控管者，收到「當事人不清楚該公司要求同意利用個資的目的」之申訴。該公司認為有需要查明當事人是否理解該公司在要求同意時提供的資訊。X依客戶分類組成自願受測小組，並在對外公布之前，將更新的同意資訊提供給這些受測人員。小組人員的挑選符合獨立性原則，並且基於確保產出結果的代表性及不帶偏見之標準。該小組收到問卷並寫下其對資訊的理解，以及對於資訊的可理解性與關聯性如何評分。控管者持續進行測試，直到小組表明該資訊已可理解。X將測試結果製成報告並保存作為未來的參考。此示例即展示X得以證明「當事人在同意X運用個資之前，已獲得清楚資訊」

[39] See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).
見前言第42點及第93/13/EC號指令，特別是第5條（簡白可理解之語言，且如有疑義，從有利於消費者之解釋）及第6條（部分條款因不公平而無效時，契約僅在除去該條款仍屬合理時始繼續有效，否則全部契約均歸無效）。

的可能方式。

[Example 13]
A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.[40] However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid "informed" consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b)GDPR.

[示例13]

某公司以同意為法律依據而運用個人資料。該公司使用階層式隱私聲明，其中包含要求給予同意。該公司揭露控管者的所有基本細節以及規劃的個資運用行為[40]。然而，該公司在聲明的第一層資訊中並未說明如何聯繫其資料保護長。基於第6條以獲得有效合法基礎為目的之規範意旨，即便未依GDPR第13條第1項第b款或第14條第1項第b款向當事人（在第一層資訊）提供資料保護長的聯絡方式，該控管者仍已取得有效的「知情」同意。

3.4. Unambiguous indication of wishes
非模糊的意思表示

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.

GDPR明確要求同意須有當事人的聲明或清楚肯定行為，此表示同意須經由積極行動或聲明而提出。當事人對特定運用行為之同意須足夠明顯。

Article 2(h) of Directive 95/46/EC described consent as an "indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action*, in line with previous guidance issued by the WP29.

95/46/EC指令第2條第h款將同意描述為一個「當事人為表明同意運用與其有關之個人資料而作出的意思表示」。GDPR第4條第11款即以此定義為基礎，說明有效同意須有一個透過*聲明或清楚肯定行為*所為的*非模糊*表示，此與WP29之前發布的指引相符。

A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing.[41] Recital 32 sets out additional guidance on this. Consent can be

[40] Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.
當控管者的身分或運用行為的目的在階層式隱私聲明的第一層資訊並不明顯時（記載於下一層），除非資料控管者可證明該當事人在給予同意前已存取該資訊，否則資料控管者將難以證明當事人已給予知情同意。

[41] See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: "As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers

collected through a written or (a recorded) oral statement, including by electronic means.
一個「清楚肯定的行為」代表當事人必須在慎重考慮後，以行動對特定運用行為表示同意[41]。前言第32點對此有額外指引。同意之蒐集可經由書面或（經記錄的）口頭聲明，包含以電子方式為之。

Perhaps the most literal way to fulfil the criterion of a "written statement" is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.
或許最符合「書面聲明」文義的標準方式即是確保當事人將其同意的內容於書面或電子郵件中寫下以交付控管者。然而這通常不夠實際。書面聲明可以多種形式和尺寸符合GDPR的要求。

Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.
在不牴觸現行（國家）契約法的前提下，雖然在當事人表示同意之前，必須充分註明當事人可得之資訊，但同意可藉由經記錄之口頭聲明而獲得。在GDPR下，使用預先勾選同意加入的框格是無效的。當事人的單純沉默、不作為或繼續使用服務之行為，均不可視為對其選擇的積極表示。

> [Example 14]
> When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, "I consent", the user is able to validly perform a ´clear affirmative act´ to consent to the processing.
> [示例14]
> 在安裝軟體時，應用程式要求當事人同意利用非匿名的當機報告以優化軟體。階層式隱私聲明提供包含同意之請求在內的必要資訊。藉由主動勾選「我同意」的框格，使用者即可有效作出一個「清楚肯定的行為」以同意運用個資。

A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes').[42]

---

is not expected to be major."
見執委會工作文件，衝擊評估，附錄2，第20頁及第105頁至第106頁：「正如WP29通過關於同意的意見書同樣指出，有必要明確說明的是，有效同意需採用對當事人之同意意思不會存有懷疑的機制，且清楚說明在線上環境中，讓當事人須更改設定才可拒絕運用的預設選項（『基於沉默的同意』），其本身並不構成非模糊的同意。此將使個人在控管者基於其同意而運用資料時，對其資料有更多的控制權。至於對資料控管者的衝擊方面，由於此僅澄清並更詳細說明現行指令關於當事人有效且有意義之同意的意旨，此將不會有重大影響。特別是取代『非模糊』的『明確』同意一詞僅在說明同意的形式與品質，且無意擴大以（明確）同意作為運用依據的適用情形，因此此方式對資料控管者的衝擊應不重大」。

[42] See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.
見第7條第2項。亦見02/2013關於為cookies獲取同意之工作文件（WP208），第3頁至第6頁。

控管者也應留意，同意不可經由「同意某契約或接受某服務之一般條款與條件所為的同一行為」而取得。對一般條款與條件的空白接受，不可視為同意使用個人資料的清楚肯定行為。GDPR並不允許控管者提出讓當事人要有介入行為才可免於同意（例如「選擇退出框格」）的預先勾選框格或選擇退出架構[42]。

When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.[43] An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.
當同意是經電子方式之請求而給予時，該請求不可*非必要地*造成服務使用上的干擾[43]。如果較低侵擾或干擾的方式將導致意義不明的話，當事人以積極肯定的行為表達同意即有必要。因此，為使同意的請求發生效力，可能有必要在某種程度上干擾使用體驗。

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.
然而在GDPR的規範下，控管者可自由發展適合其組織的同意流程。在這點上，身體動作可符合GDPR規範的清楚肯定行為。

Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.
控管者應以對當事人足夠清晰的方式設計同意機制。控管者必須避免任何模糊空間，並確保給予同意之行為可與其他行為有所區別。因此，僅是持續一般的使用網站並不可推論為當事人對運用行為表達同意的意思表示。

[Example 15]
Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.
[示例15]
只要已提供清楚的資訊，且該動作可清楚表明對特定請求的同意（例如將捲軸滑至左方，即表示同意基於Y目的而利用X資訊。重複該動作以確認），則滑動螢幕上的捲軸、在智慧鏡頭前揮手、將智慧型手機順時鐘或八字形旋轉，均是表示同意的選項。控管者必須證明以此方式獲得同意，且當事人可以同樣簡易方式撤回同意。

[Example 16]
Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action.

[43] See Recital 32 GDPR.
見GDPR前言第32點。

This is because the alert that continuing to scroll will constitute consent may be difficult to distinguish and/or may be missed when a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

[示例16]

下捲或滑過網站無法滿足清楚及肯定行動的要求。這是因為對於繼續瀏覽即構成同意的警示可能不易辨認，且/或在當事人快速瀏覽大量文字時恐遭忽略，進而使該行為有模糊空間。

In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.

在數位環境下，許多服務需要個人資料以提供功能，因此，當事人每天收到多個需要點擊或滑動以回覆的同意請求。這可能造成某程度的點擊疲勞：即遇到越多次時，同意機制真正的警示效果就越趨減損。

This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.

這導致大家不再閱讀關於同意的提問。此對當事人尤其是個風險，因為在典型的情況，徵求同意是為了未獲得同意即屬違法的行為。GDPR課予控管者想出方法以茲因應的義務。

An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

對此，線上環境有個常被提及的因應實例，即經由瀏覽器設定以取得網路使用者的同意。此類設定應遵循GDPR對於有效同意的條件而設計，例如同意應分別針對各個預想的目的，以及提供的資訊中應包含控管者的名稱。

In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity.[44] Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording "has given" in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject's consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

無論如何，如獲得同意是控管者運用個人資料所必須，控管者應在運用個資之前取得該同意。WP29在先前的意見中一致地認為，同意應在運用行為之前提供[44]。雖然GDPR在第4條第11款的文字中並未規定同意須在運用行為之前給予，但已清楚揭示此意。第6條第1項的條文名稱以及第6條第1項第a款的文字「已給予」即足支持此解釋。由第6條及前言第40點的邏輯推

[44] WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.
WP29自15/2011關於同意的定義之意見書（WP187），第30頁至第31頁以來一貫保持此見解。

演可知，有效的合法基礎必須在開始運用個資之前即已存在。因此，同意應在運用行為之前給予。原則上，向當事人請求一次同意即為已足。然而，控管者如在取得同意後變更運用個資之目的，或規劃額外的目的時，即須取得一個新的特定同意。

4. Obtaining explicit consent
獲得明確同意

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49[45] , and in Article 22 on automated individual decision-making, including profiling.[46]
在有重大個資保護風險情形出現時，明確同意有其必要，因此，宜針對個人資料提供高度個人掌控權。在GDPR規範下，明確同意出現在第9條關於特種個資的運用、第49條關於在缺少充分防護措施的情形下，將個資傳輸至第三國或國際組織的規範[45]，以及第22條關於包含建檔在內的自動化個人決定[46]等條文中。

The GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for 'regular' consent. As the 'regular' consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.
GDPR將「聲明或清楚肯定的行動」規定為「一般」同意的必要條件。由於GDPR對於「一般」同意的規範相較95/46/EC指令已有更高標準，因此有必要澄清控管者應採取何種額外措施獲得當事人的*明確*同意以符合GDPR。

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[47]

---

[45] According to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.
依GDPR第49條第1項第a款規定，明確同意可解除禁止將資料傳輸至不具備適足程度之資料保護法律的國家。也留意關於1995年10月24日之95/46/EC指令第26條第1項的共通解釋之工作文件（WP114），第11頁，WP29在此指出，以同意作為對週期性或持續性的資料傳輸之依據並不恰當。

[46] In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2)(c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject's explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).
在第22條中，GDPR提出保護當事人免於僅根據自動化運用行為（包含建檔）而作出決定之條款。在特定條件下才可依此作出決定。同意在這個保護機制中扮演重要角色，即GDPR第22條第2項第c款清楚規定控管者可根據當事人的明確同意而採行對個人可能有重要影響的自動化決定，包含建檔。WP29對此議題個別提出指引：WP29關於依第2016/679號規則之目的的自動化決定與建檔之指引，2017年10月3日（WP251）。

[47] See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.
見WP29 15/2011意見書關於同意的定義（WP187），第25頁。

*明確*一詞涉及當事人表達同意的方式。此代表當事人必須作出明確聲明來表示同意。確保同意明確的一種明顯方式是藉由書面聲明明確地確認其同意。在適當的情形下，控管者可確保當事人在該書面聲明中簽名，以避免所有可能的質疑及將來潛在無法舉證的情況[47]。

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.

然而，簽名的聲明並非取得明確同意的唯一方式，且GDPR並未規定在所有需要有效的明確同意之情形，都要有書面簽名的聲明。舉例來說，在數位或線上環境下，當事人可透過填寫電子表格、寄送電子郵件、上傳包含當事人簽名在內的掃描後文件，或使用電子簽章以提交所需的聲明。理論上，口頭聲明對於取得有效的明確同意也足夠明確，不過，控管者在記錄該聲明時，可能不易舉證已符合所有有效的明確同意之條件。

An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).

只要相關選項的資訊足夠公平、可理解、夠清楚，且向當事人要求具體的確認動作（例如按下按鈕或提供口頭確認），組織也可經由電話對話而獲得明確同意。

> [Example 17] A data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance "I, hereby, consent to the processing of my data", and not for instance, "It is clear to me that my data will be processed". It goes without saying that the conditions for informed consent as well as the other conditions for obtaining valid consent should be met.
>
> [示例17]藉由在獲得明確同意的螢幕上提供是、否勾選框格，只要文字清楚指出同意，例如「我在此同意對我的個人資料之運用行為」，而非例如「我清楚我的個人資料將被運用」，則資料控管者也可以此獲得網站訪客的明確同意。但仍須符合知情同意及其他獲得有效同意之條件，自不待言。

> [Example 18] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.[48]
>
> [示例18]某整形診所為向專家就病人的情況尋求第二意見而請求病人明確同意傳輸其醫療紀錄。該醫療紀錄為數位檔案。考量該資訊的特定性質，該診所要求當事人提供電子簽章以獲得有效的明確同意，並可證明已取得該明確同意[48]。

Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a

[48] This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
此示例不牴觸歐洲議會與歐盟理事會2014年7月23日關於內部市場電子交易之電子身分驗證及信賴服務的歐盟規則（EU）第910/2014號。

record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.
雙階段驗證同意也可作為確保明確同意之有效性的方式。舉例來說，當事人收到一封電子郵件通知信，說明控管者有意運用包含醫療資料在內的紀錄。該控管者在信中解釋，其基於特定目的而請求同意使用特定的資訊。如當事人同意其使用個人資料，控管者要求以電子郵件回覆「我同意」之聲明。當事人在寄出回覆後，即收到必須點選的驗證連結，或含有驗證碼在內的簡訊，以此確認同意。

Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.
第9條第2項未將「為履行契約所必要」列為禁止運用特種個資的例外條款。因此控管者及成員國對此應探究第9條第2項第b款至第j款的特殊例外規定。若第b款至第j款均不適用時，遵守GDPR對有效同意之條件以獲得明確同意，將成為運用該類個資唯一可能的合法例外。

[Example 19]
An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to a disability. A customer books a flight from Amsterdam to Budapest and requests travel assistance to be able to board the plane. Holiday Airways requires her to provide information on her health condition to be able to arrange the appropriate services for her (hence, there are many possibilities e.g. wheelchair on the arrival gate, or an assistant travelling with her from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. -The data processed on the basis of consent should be necessary for the requested service. Moreover, flights to Budapest remain available without travel assistance. Please note that since that data are necessary for the provision of the requested service, Article 7 (4) does not apply.
[示例19]
假期航空公司為無法自行旅行的乘客（例如因為身心障礙）提供旅行協助服務。某顧客預訂從阿姆斯特丹飛往布達佩斯的航班，並要求提供旅行協助以順利登機。假期航空要求該顧客提供關於健康情形的資訊以妥善安排服務（因此有許多選項，例如接機口的輪椅或從阿姆斯特丹到布達佩斯的陪伴飛行助手）。假期航空基於安排旅行協助的目的而要求該顧客給予運用健康資料的明確同意。基於同意而運用之個人資料對於所要求的服務應有必要。此外，飛往布達佩斯但不提供旅行協助的航班仍有空位。請留意，既然該個人資料對所要求提供的服務係屬必要，第7條第4項在此即不適用。

[Example 20]
A successful company is specialised in providing custom-made ski- and snowboard goggles, and other types of customised eyewear for outdoors sports. The idea is that people could wear these without their own glasses on. The company receives orders at a central point and delivers products from a single location all across the EU. In order to be able to provide its customised products to customers who are short-sighted, this controller requests consent for the use of information on customers' eye condition. Customers provide the necessary health data, such as their prescription data online when they place their order. Without this, it is not possible to provide the requested customized eyewear. The company also offers series of goggles with standardized correctional values. Customers that do not wish to share health data could opt for the standard versions.

Therefore, an explicit consent under Article 9 is required and consent can be considered to be freely given.

[示例20]

某間成功的公司專門提供客製化的滑雪板及護目鏡，以及其他類型客製化戶外運動眼鏡。人們戴上該公司產品即不用再戴自己的眼鏡。該公司集中接受訂單，並從單一據點向全歐盟寄送產品。為提供客製產品給近視的顧客，該控管者要求同意使用關於顧客視力情況的資訊。顧客在線上下訂時提供了必要的健康資料，例如處方資料。如果沒有此類資料，將無法提供所要求的客製化眼鏡。該公司同時提供一系列標準度數的護目鏡。不願分享健康資料的顧客可以選擇標準版產品。因此，此處須要第9條規定的明確同意，而該同意可視為自由給予。

5. Additional conditions for obtaining valid consent
獲得有效同意的其他條件

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.

GDPR規範控管者採取額外措施以確保其獲得、維持，並可證明有效同意。GDPR第7條藉由同意紀錄之保存與輕易撤回同意之權利等特別條款，以訂定這些針對有效同意的額外條件。第7條也適用於GDPR其他涉及同意之條文，例如第8條及第9條。以下即就證明有效同意的額外規範以及關於同意之撤回提供指引。

5.1. Demonstrate consent
證明同意

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

在第7條第1項中，GDPR清楚指出控管者負有證明當事人同意的明確義務。依第7條第1項規定，此應由控管者負舉證責任。

Recital 42 states: *"Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation."*

前言第42點謂：「*當運用的依據為當事人之同意時，控管者須能證明該當事人已對該運用作業給予同意*」。

Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

控管者可採適合其日常作業的方式，自由發展遵循該條款的方法。在此同時，控管者有責任證明其獲得有效同意，但該責任不應導致過量運用其他資料。這表示控管者應有足夠的資料來證明與運用行為之間的連結（證明已獲得同意），但不可在必要範圍外蒐集任何更多的資訊。

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR

does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and (e).
控管者可決定如何證明已自當事人獲得有效同意。GDPR並未明確規定該如何滿足此義務。然而，控管者須能證明在個案中的當事人已表示同意。只要系爭資料運用行為持續存在，證明同意的義務便持續存在。依第17條第3項第b款及第e款規定，在運用行為終了後，同意證據的保存期限不應超過遵守法律義務或建立、行使或防禦法律上請求所需的嚴格必要範圍。

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller´s workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.
舉例來說，控管者可以保存所收到的同意聲明之紀錄，以便在需要舉證時，證明如何獲得同意、何時獲得同意，以及當時曾提供給當事人的資訊為何。控管者也須能證明當事人的知情，以及控管者的工作流程符合所有有效同意的相關標準。此義務在GDPR中的背後原理在於，控管者對於自當事人獲得有效同意以及其採取的同意機制應負責任。例如，在線上環境中，控管者可將表達同意的連線進程資訊予以保存，併同該連線進程進行時的同意工作流程之文件紀錄，以及當下提供予當事人之資訊的複本（檔）一併保存。僅是提出個別網站的正確組態設定並不足夠。

> [Example 21] A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.
> [示例21]某醫院發起一個名為X計畫的科學研究計畫，需要實際的病人牙科紀錄。該計畫招募參與者的方式為致電病人，詢問是否同意自願加入候選名單，以便依此目的向其聯繫。控管者向當事人尋求明確同意使用牙科紀錄。此同意是經由錄下當事人確認同意為X計畫之目的使用其個資的口頭聲明，而在電話中獲得。

There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.
GDPR對於同意的有效期限沒有特別限制。同意的效期應視個案背景、原始同意的範圍以及

當事人的期待而定。如運用作業有相當大的變更或演變，則原本的同意即不再有效。在此情形便須要獲得新的同意。

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.[49]
WP29對最佳實務的建議是，同意應適時更新。再次提供全部資訊有助於確保當事人對於其資料如何被使用以及如何行使其權利，能保持良好的知情狀態[49]。

5.2. Withdrawal of consent
撤回同意

Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.[50]
同意之撤回在GDPR佔有重要地位。GDPR中關於同意之撤回的條款與前言，可視為是WP29意見中對此議題現有之解釋的彙整[50]。

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.
GDPR第7條第3項規定，控管者應確保同意可由當事人以給予同意相同簡易的方式，在任何時間撤回。GDPR並未規定給予和撤回同意必須透過同樣動作完成。

However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.[51]
然而，當同意是以一鍵點擊滑鼠、滑動或按鍵等電子方式獲得時，當事人在實作上須可以相同簡易的方式撤回該同意。如同意是藉由使用該服務特定的使用者介面（例如透過網站、應用程式、登入帳號、物聯網裝置的介面或電子郵件）而獲得時，當事人毫無疑問須可以相同的電子介面撤回同意，因為僅是為了撤回同意而須切換至其他介面將需要過度付出。此外，

[49] See WP29 guidelines on transparency. [Citation to be finalized when available]
見WP29關於透明化之指引。[將於可得時確定引註內容]

[50] WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).
WP29曾於關於同意之意見書（見15/2011關於同意的定義之意見書（WP187），第9頁、第13頁、第20頁、第27頁及第32頁至第33頁）及特別是關於位置資料的使用之意見書（見5/2005關於由提供加值服務的觀點探討位置資料的使用之意見書（WP115），第7頁）中討論此主題。

[51] See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).
見WP29 4/2010關於在行銷中使用個人資料之歐洲FEDMA行為守則之意見書（WP174）以及關於由提供加值服務的觀點探討位置資料的使用之意見書（WP115）。

當事人須可不受損害的撤回同意。這意味控管者尤應盡可能使撤回同意無需付費或不致降低服務水平[51]。

> [Example 22] A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.
>
> [示例22]某音樂節透過線上票券代理商銷售門票。在每一次線上販售票券時，均針對基於行銷目的利用其聯絡方式，尋求(顧客)同意。針對此目的，顧客可選擇不同意或同意，且控管者通知顧客有權撤回同意，如欲行使該權利，可在營業日的早上8點到下午5點間致電客服中心，不須給付任何費用。本例中的控管者並未符合GDPR第7條第3項規定。在本例中，相較於24小時均可透過線上票券販售商以一鍵點擊滑鼠方式給予同意，須在營業時間撥打電話才可撤回同意，較為麻煩。

The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1 on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.[52]
GDPR將簡易撤回的規範定性為有效同意的必要部分。若撤回權利未達到GDPR之要求，控管者的同意機制即不符合GDPR規範。如同在第3.1段關於*知情*同意之條件所述，按照GDPR第7條第3項規定，控管者應在當事人給予同意之前即告知其有撤回同意之權利。此外，控管者基於透明化義務，應告知當事人該如何行使權利[52]。

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.[53]
基於一般法理並依GDPR規定，同意經撤回後，所有依據同意而為的資料運用行為以及在撤回前已發生的同意均仍屬合法，然而，控管者應即終止該運用動作。若無其他合法基礎合法化資料運用行為（例如繼續儲存），控管者應將資料刪除[53]。

As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore

[52] Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.
討論本規則第13條及第14條的GDPR前言第39點謂「自然人應受告知有關個人資料運用之風險、規則、安全維護及權利，以及如何行使與該運用行為有關之權利」。

[53] See Article 17(1)(b) and (3) GDPR.
見GDPR第17條第1項第b款及第3項。

be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.
本指引前已提及，控管者在蒐集資料之前即評估運用資料之目的及所依據的合法事由一事至為重要。公司經常基於數個目的需要個人資料，並依不只一種合法基礎而運用，例如基於契約和同意而運用顧客資料。因此，撤回同意並不表示控管者須要刪除基於履行與當事人間的契約之目的而運用的資料。控管者應自始清楚掌握適用於各個資料之目的以及其合法基礎。

Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention.[54] Besides this situation, covered in Article 17 (1)(b), an individual data subject may request erasure of other data concerning him that is processed on another lawful basis, e.g. on the basis of Article 6(1)(b).[55] Controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.[56]
假如沒有其他目的可合法化持續保存行為時，控管者有義務在同意經撤回後即刪除基於同意而運用之資料[54]。除此情形之外，依第17條第1項第b款內容，個別當事人可請求刪除基於另一個合法基礎而運用的與其有關之其他資料，例如依據第6條第1項第b款[55]。即便當事人未請求刪除，控管者仍有義務評估繼續運用系爭資料是否適當[56]。

In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.
如當事人撤回同意而控管者仍欲以另一個合法基礎繼續運用個人資料時，控管者不可私下將同意（已被撤回）移轉至其他合法基礎。任何運用行為合法基礎的變更均應依照第13條及第14條對於資訊揭露的規範以及透明化的通常原則來通知當事人。

6. Interaction between consent and other lawful grounds in Article 6 GDPR
同意與GDPR第6條其他合法基礎的適用關係

Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.[57]
第6條規定合法運用個資的要件，並設有6種控管者可依據的合法基礎。此6種合法基礎的適用必須在運用行為之前即已存在，且應與特定目的具備關聯性[57]。

It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an

[54] In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.
在此情形，其他可合法化運用行為之目的必須自行具備個別的法律基礎。這不表示控管者可任意由同意變更至另一個合法基礎，見下方第6部分。

[55] See Article 17, including exceptions that may apply, and Recital 65 GDPR
見第17條，包含可適用的例外，以及GDPR前言第65點

[56] See also Article 5 (1)(e) GDPR
見GDPR第5條第1項第e款

[57] Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.
依第13條第1項第c款及/或第14條第1項第c款規定，控管者應將此告知當事人。

individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals.
在此有必要說明，如控管者選擇以同意作為任何一部分運用的依據，即應重視該選擇，並對當事人撤回同意後即終止該部分之運用有所準備。如對外表示依據同意而運用資料，但實際上卻是依據其他的合法基礎時，將對個別當事人構成本質上的不公平。

In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.
換句話說，控管者不可將同意與其他合法基礎互換。舉例而言，當同意的有效性遇到問題時，不允許為了合法化運用行為而溯及適用正當利益作為依據。基於在蒐集個資的當下即應揭露控管者依據的合法基礎之規範，控管者應於蒐集之前即決定適用的合法依據。

7. Specific areas of concern in the GDPR
GDPR中的特定領域考量

7.1. Children (Article 8)
兒童（第8條）

Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: *" [...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]"* Recital 38 also states that "*Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."* The words 'in particular' indicate that the specific protection is not confined to marketing or profiling but includes the wider 'collection of personal data with regard to children'.
相較於現行(95/46/EC)指令，GDPR針對特別是兒童等弱勢自然人的個資運用創設額外的保護層級。第8條對於資訊社會服務提出額外的義務，以確保強化兒童資料保護的等級。強化保護的理由載明於前言第38點：「*...他們對於風險、結果、有關的安全措施以及他們享有關於個資運用之權利等，可能較缺乏認知...*」。前言第38點也說明「*這類特定保護措施應尤其適用在基於行銷、建立人格或使用者檔案等目的而對兒童個人資料的利用行為，以及在使用直接對兒童提供之服務時，對兒童個人資料的蒐集行為*」。「尤其」一詞表示該特定保護措施並不限於行銷或建檔，尚包含更廣泛的「對兒童個人資料的蒐集行為」。

Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility

over the child.[58] Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.
第8條第1項表明，在直接向兒童提供資訊社會服務的情形，如適用同意時，該兒童須至少年滿16歲，運用該兒童的個人資料才屬合法。當該兒童未滿16歲時，該運用僅在兒童的法定代理人給予或授權之同意範圍內始屬合法[58]。GDPR對於有效同意的年齡限制提供彈性，成員國可以法律制定較低的年齡門檻，但不得低於13歲。

As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain "informed consent" from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.[59] If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.
如同第3.1節關於知情同意所述，控管者對受眾提供的資訊應可得理解，且應特別考量兒童的立場。為了向兒童獲得「知情同意」，控管者必須使用對兒童來說清楚而簡白的語言，解釋將如何運用所蒐集的資料[59]。如果是應由家長同意的情形，可能便需要提供能讓成年人做出知情決定的一連串資訊。

It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:
- The processing is related to the offer of information society services directly to a child.[60,61]
- The processing is based on consent.

由前述內容可知，第8條僅在滿足下列條件時始有適用：
- 該運用與直接向兒童提供資訊社會服務有關[60, 61]。
- 該運用是以同意為依據。

7.1.1. Information society service
資訊社會服務

To determine the scope of the term 'information society service" in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

[58] Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).
無礙於成員國以法律降低年齡限制，見第8條第1項。

[59] Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.
GDPR前言第58點重申此義務，謂在適當時，控管者應確保提供予兒童的資訊可得理解。

[60] According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: "(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request." An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.
根據GDPR第4條第25款規定，資訊社會服務依第2015/1535號指令第1條第1項第b款定義為：「(b)『服務』指任何資訊社會服務，也就是任何通常以電子方式提供的遠距而有償之服務，且屬於依接受服務者個別請求而提供之服務。為此定義之目的：(i)『遠距』意指提供該服務無須雙方同時在場；(ii)『以電子方式』意指該服務藉由電子設備發送及接受以運用（包含數位壓縮）並儲存資料，且完全透過有線、無線、光學方法或其他電磁方法而傳輸、傳達與接收；(iii)『依接受服務者個別請求』意指該服務係藉由傳輸資料之個別請求而提供」。該指令將不包含於此定義之服務列於附件1。亦見第2000/31號指令前言第18點。

[61] According to the UN Convention on the Protection of the Child, Article 1, "[…] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier," see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).
根據聯合國兒童權利公約第1條，「[…]兒童係指未滿18歲之人，但該兒童適用之法律有較早成年之規定者從其規定」見聯合國1989年11月20日第44/25號大會決議（兒童權利公約）。

為了決定GDPR所稱「資訊社會服務」的範圍，GDPR第4條第25款即規定應參照適用2015/1535指令。

While assessing the scope of this definition, WP29 also refers to case law of the ECJ.[62] The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.
在評估此定義的範圍時，WP29條同時參考歐洲法院的判例法[62]。歐洲法院認為，*資訊社會服務*包含在線上締結或傳送的契約和其他服務。當某服務包含兩個經濟上獨立的要素，其一是線上要素，例如為締結契約所為的要約與承諾行為，或是提供與產品或服務有關之資訊，包含行銷活動，此要素即定義為資訊社會服務。另一要素為實體的商品寄送或銷售，則不包含在資訊社會服務的概念中。線上提供的服務則涵蓋於GDPR第8條所稱*資訊社會服務*的範圍。

7.1.2. Offered directly to a child
直接對兒童提供

The inclusion of the wording 'offered directly to a child' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.
條文中包含「直接對兒童提供」，代表第8條僅欲適用於某些資訊社會服務。就此而言，如果資訊社會服務提供者清楚向潛在使用者表示其僅提供服務予18歲以上之人，且無其他證據（例如網站內容或行銷計畫）顯示相反情形，則該服務將不被認為是「直接對兒童提供」，第8條即不適用。

7.1.3. Age
年齡

The GDPR specifies that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."* The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to

[62] See European Court of Justice, 2 December 2010 Case C-108/09, (Ker-Optika), paragraphs 22 and 28. In relation to 'composite services', WP29 also refers to Case C-434/15 (AsociacionProfesional Elite Taxi v Uber Systems Spain SL), para 40, which states that an information society service forming an integral part of an overall service whose main component is not an information society service (in this case a transport service), must not be qualified as 'an information society service'.
見歐洲法院2010年12月2號C-108/09判決，（Ker-Optika），第22段及第28段。關於「綜合服務」部分，WP29亦參考C-434/15 (Asociacion Profesional Elite Taxi v Uber Systems Spain SL)判決，第40段，該段謂若一項資訊社會服務是某完整服務的一部分，但該完整服務的主要內容並非資訊社會服務（本案即指交通運輸服務）時，即不滿足「資訊社會服務」之要件。

comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.
GDPR明確指出「*成員國可以法律為該目的訂定較低的年齡限制，但不可低於13歲*」。控管者應考量其服務鎖定之對象而留意不同國家的法律。應特別說明的是，提供跨境服務的控管者無法僅遵守其主要據點所在地的國家法律，而可能需要遵守其提供資訊社會服務所及的各個國家的各別法律。這取決於該成員國選擇以控管者的主要營業據點所在地或當事人的居住地作為適用內國法律的判斷依據。成員國在選擇時，首要考慮兒童的最佳利益。工作組鼓勵成員國就此議題尋找調和的解決方案。

When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.
在以同意為依據而對兒童提供資訊社會服務時，控管者被期待採取合理的努力去驗證以電子方式同意的使用者已超過年齡標準，且這些措施與運用行為的性質與風險間應符合比例原則。

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.
如使用者聲稱已超過電子方式同意的年齡，控管者即可以適當查驗方式驗證該聲明是否真實。雖然GDPR並未明確要求須採取合理的努力以驗證年齡，但仍隱含寓有此意，因為如果未達到能自行提供有效同意之年齡標準的兒童給予同意時，將導致資料運用違反法律。

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.
如使用者聲稱未達到電子方式同意的年齡，控管者可無須進一步查驗而接受該聲明，但將需要再獲得家長授權，且須驗證提供該同意之人為法定代理人。

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.[63] If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.[64]
驗證年齡不應導致過度的資料運用。驗證當事人年齡的機制應包含對運用行為的風險評估。

[63] Although this may not be a watertight solution in all cases, it is an example to deal with this provision
雖然這可能不是最嚴謹的解決方案，但不失為因應本條規範的示例
[64] See WP29 Opinion 5/2009 on social networking services (WP 163).
見WP29意見5/2009關於社會網路服務（WP163）。

在某些低風險情形，要求服務的新訂戶揭露其出生年份或填寫表格聲明「非」未成年人，可能是適當的[63]。如有疑慮時，控管者應在具體個案審查其年齡驗證機制，並考慮是否需要替代的查驗方式[64]。

7.1.4. Children's consent and parental responsibility
兒童同意與法定代理權

Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.[65] Therefore, the WP29 recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

對於法定代理人的授權，GDPR並未明確規定取得父母同意或建立有權行使該行為的實務作法[65]。因此，WP29建議依照GDPR第8條第2項及第5條第1項第c款（資料最小化）之意，採取符合比例原則的方法為之。符合比例原則的方法或許可著重於僅取得有限的資訊，例如父母或監護人的聯絡方式。

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.[66] Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

對於「使用者的年齡已足夠自行提供同意」與「代表兒童提供同意之人確實為法定代理人」之驗證方式是否合理，可能取決於運用造成的風險以及可得的技術而定。在低風險案例，以電子郵件驗證法定代理權可能即已足夠。相對地，在高風險案例，要求更多的證據可能較為妥當，這樣控管者才可驗證並依GDPR第7條第1項規定保存資訊[66]。受信任之第三方驗證服務或可提供解決方案，最少化控管者須自行運用的個人資料。

> [Example 23] An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:
> Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent)
> If the user states that they are under the age of digital consent:
> Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.
> Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.

[65] WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.
WP29指出，並非所有法定代理人均為該兒童的原生父母，且該法定代理權可由包含法人與自然人在內的多方共同行使。

[66] For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.
例如可要求父母或監護人透過銀行交易給付控管者0.01歐元，並在交易的描述列記載該銀行帳戶持有人為該使用者之法定代理人的簡要確認聲明。如適當時，應向未持有銀行帳戶之人提供驗證身分的替代方案，以避免不當的差別待遇。

Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.
If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

[示例23]某線上遊戲平台要確保未達年齡限制的客戶僅在父母或監護人同意的情形下訂購服務。該控管者遵循下列步驟：

步驟1：要求使用者聲明是否低於或高於16歲（或以電子方式同意的其他年齡限制）。如使用者聲稱未達使用電子方式同意的年齡：

步驟2：該服務提醒兒童，在向其提供服務之前，需要有父母或監護人的同意或授權。該使用者被要求提供一位父母或監護人的電子郵件信箱。

步驟3：該服務與該父母或監護人聯繫，並透過電子郵件取得其對運用的同意，且以合理步驟確認該成年人是法定代理人。

步驟4：如有申訴情形，該平台即採取額外步驟驗證訂戶的年齡。

如該平台滿足同意的其他規範，即可依循上述步驟遵守GDPR第8條的額外標準。

The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that "*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology."*

此示例顯示，控管者在向兒童提供服務時，證明自己已做出合理的努力以確保獲得之同意為有效。第8條第2項特別加入「*控管者應做出合理的努力，考量在既有技術的情況下，驗證同意是由該兒童的法定代理人給予或授權*」。

It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.

控管者可自行決定特定個案中的適當方式。原則上，控管者應避免需要過度蒐集個人資料的驗證方案。

WP29 acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an 'identity footprint', or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.

WP29瞭解有些情形可能難以執行驗證（例如尚未建立「身分足跡」而自行提供同意的兒童，或無法輕易查驗法定代理權的情形。在決定何種努力屬於合理時，可將這類情形納入考量，但控管者也被期待持續檢視其運用行為與可得技術。

With regard to the data subject's autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent.

In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data given prior to the age of digital consent, will remain a valid ground for processing.

After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.[67]
在當事人同意運用其個人資料的自主性以及對於運用的完整控制方面，原本由法定代理人對運用兒童的個人資料所為之同意或授權，當事人一旦達到電子方式同意的年齡門檻後，即可確認、修改或撤回。
實務上，這表示如該兒童並未採取任何行動，則在達到電子方式同意的年齡限制之前已由法定代理人對運用兒童的個人資料所為之同意或授權，仍將成為運用的有效依據。
在達到電子方式同意的年齡門檻後，該兒童將有可能依第7條第3項撤回同意。基於公平性與課責性原則，控管者應告知該兒童有關撤回同意的選擇[67]。

It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.
在此有必要指出，依照前言第38點規定，直接對兒童提供的預防性或諮詢性服務即不需要父母或監護人的同意。舉例來說，藉由線上對話服務的方式，在線上對兒童提供保護的服務便不需要家長事前授權。

Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with "the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child". Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.
最後，GDPR強調，有關未成年人的家長授權之規定不應妨礙「成員國之一般契約法，例如關於兒童之契約效力、形式或效果」。因此，獲得有效同意以利用兒童資料的規範係法律框架的一部分，須與內國契約法律區分視之。故本指引文件並不處理未成年人締結線上契約是否合法的問題。兩種法律制度可能同時適用，且GDPR的範圍並不包含調和各國的契約法律規範。

7.2. Scientific research
科學研究

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term *'scientific research'* is not defined in the GDPR. Recital 159 states "(…) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (…)", however the WP29 considers the notion may not be stretched beyond its common meaning and understands that '*scientific research'* in this context means a research project set up in accordance with relevant

[67] Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.
同時，當事人應獲知第17條規定的被遺忘權，此在給予同意的當事人仍為兒童時尤其重要，見前言第63點。

sector-related methodological and ethical standards, in conformity with good practice.
科學研究目的之定義對於控管者可從事的資料運用行為之範圍具有重大影響。GDPR並未定義「*科學研究*」一詞。前言第159點謂「（...）*基於本規則之目的，應以寬鬆方式解釋為科學研究目的而運用個人資料。*（...）」然而WP29認為不應將其概念延伸至通常意義之外，並瞭解在此脈絡下的「*科學研究*」意指符合相關領域之方法論及倫理標準，且遵循優良實務的研究計畫。

When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard.[68] At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.[69] This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).[70]
當依照GDPR規定而以同意作為進行研究的法律依據時，針對使用個人資料的同意應與其他針對倫理標準或程序義務所需要的同意有所區別。在臨床試驗規則中即可找到程序義務的示例，此時運用行為並非以同意為依據而是其他的法律基礎。在資料保護法律的背景下，後者形式的同意可視為一種額外的安全措施[68]。在此同時，GDPR並未限制適用第6條規定僅以同意作為基於研究目的而運用資料之依據。只要存有適當安全維護，例如第89條第1項的規範，且該運用具備公平性、合法性、透明化，並與資料最小化標準與個人之權利具備一致性，其他例如第6條第1項第e款或第f款的合法依據也可能適用[69]。此亦適用於第9條第2項第j款對特種個資所設之例外條款[70]。

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*."
前言第33點對於科學研究中的同意之特定性與區別性提供些許彈性。前言第33點謂：「*通常不太可能在資料蒐集時便完整識別為科學研究而運用個人資料之目的。因此，如符合科學研究公認的倫理標準時，應允許當事人僅就特定範圍的科學研究給予同意。當事人應有機會僅對特定研究範圍或預期目的允許範圍內的部分研究計畫給予同意*」。

[68] See also Recital 161 of the GDPR.
見GDPR前言第161點。

[69] Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.
第6條第1項第c款也可適用於法律特別要求的部分運用行為，例如在臨床試驗規則下，遵守成員國許可的計畫而蒐集可信賴及可靠之資料。

[70] Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).
依第9條第2項第i款規定，可基於歐盟或國家法律的規定而對藥品為特定測試。

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.
首應說明的是，前言第33點非謂無須適用關於特定同意之規範的義務。其意指原則上僅在詳實描述目的之前提下，科學研究計畫才可以同意為依據而將個人資料包含在內。在一開始無法明確指出科學研究計畫所涉及資料運用目的之情形，前言第33點例外允許以較籠統的程度描述該目的。

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.
考量到GDPR第9條關於運用特種個資的嚴格條件，WP29指出，在以明確同意為依據而運用特種個資的情況，當適用前言第33點所述較有彈性的方法時，應採取較嚴格的解釋，且需要高強度的監督。

When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.
整體而言，GDPR不允許控管者規避向當事人指明目的以取得同意之重要原則。

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.
當無法完整指明研究目的時，控管者應尋求其他方式以確保最大程度滿足同意的規範意旨，例如允許當事人以較概略方式同意研究目的，以及同意一開始即知的研究計畫之特定階段。隨著研究的進展，便可在下一階段開始前獲得對該計畫後續步驟的同意。不過，該同意仍應符合科學研究適用的倫理標準。

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject*." Data minimization, anonymisation and data security are mentioned as possible safeguards.[71] Anonymisation is the preferred solution as

[71] See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality.
For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose." […] As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles."
示例見前言第156點。為科學目的運用個人資料也應遵守其他相關法律，例如有關臨床試驗之法律，前言第156點提及歐洲議會

soon as the purpose of the research can be achieved without the processing of personal data.
除此之外，控管者在此類個案中可採取進一步的安全維護。舉例來說，第89條第1項強調在為科學、歷史或統計目的而運用資料行為中的安全維護需求。這些目的「*應依本規則規定而有適當的安全維護，以保障當事人的權利與自由*」。資料最小化、匿名化以及資料安全是被提及可能的安全維護措施[71]。一旦不再需要運用個人資料也能達成研究目的時，匿名化將是較佳的解決方案。

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).[72]
當該研究無法取得特定同意時，透明化即為一個額外的安全維護措施。目的特定性的不足可經由控管者在研究計畫進行中定期告知目的之最新發展資訊而補足，隨著時間經過，同意將將越來越明確。在過程中，當事人至少對現況能有基本的理解，以供其評估是否行使例如第7條第3項的撤回同意權[72]。

Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.[73] This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.
同時，在當事人同意之前便提供詳盡的研究計畫供其留意，亦可彌補目的特定性的不足[73]。該研究計畫應盡可能明確記載研究議題與預計的執行方法。此研究計劃亦有助於遵守第7條第1項規定，因為控管者必須能提出當事人在同意的當下取得哪些資訊，以便證明該同意之有效性。

It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this –there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.[74]

與歐盟理事會2014年4月16日關於為人體使用藥物之臨床試驗的歐盟第536/2014號規則。亦見WP29 15/2011關於同意的定義之意見書（WP187），第7頁：「此外，取得同意並不免除控管者在第6條下有關公平性、必要性、合比例性，以及資料品質等義務。舉例來說，即便基於使用者同意而運用個資，亦無法合法化超出特定目的所為的資料蒐集。[…]原則上，不可將同意視為其他資料保護原則的豁免，而應視為一種安全維護。同意主要是一項合法基礎，並不免除其他原則的適用」。

[72] Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.
其他透明化措施也可能相關。當控管者基於科學目的而運用個資，但無法在一開始便提供完整資訊時，控管者可為當事人指派特定聯絡人以處理詢問。

[73] Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (Henkilötietolaki, 523/1999)
在現行芬蘭個人資料保護法（Henkilötietolaki, 523/1999）第14條第1項可見相關適用。

[74] See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

在此有必要重申，當以同意作為運用的合法依據時，當事人必須能夠撤回同意。WP29指出，撤回同意可能會對需與個資相連結的科學研究類型有所損害，然而GDPR清楚規定同意可被撤回，而控管者的行為必須受其拘束，此規範對於科學研究並無例外。當控管者收到撤回請求時，即使其有意繼續基於研究目的而使用資料，原則上即應立刻刪除個人資料[74]。

7.3. Data subject's rights
當事人權利

If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.
如某資料運用行為是以當事人之同意為依據，此將影響該當事人的權利。當運用是以同意為依據時，當事人享有個資可攜權（第20條）。同時，拒絕權（第21條）並不適用在以同意為依據而運用的情形，雖然可隨時撤回同意的權利可提供類似效果。

Articles 16 to 20 of the GDPR indicate that (when data processing is based on consent), data subjects have the right to erasure when consent has been withdrawn and the rights to restriction, rectification and access.[75]
GDPR第16條至第20條表明（當以同意作為運用資料之依據時），當事人有權在撤回同意後請求刪除資料，並有權限制、修改及近用資料[75]。

8. Consent obtained under Directive 95/46/EC
在95/46/EC指令下獲得之同意

Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.
對於目前遵守國家資料保護法律而以同意為運用資料之依據的控管者來說，並不需要因為因應GDPR而更新所有與當事人間現有的同意關係。只要與GDPR規定的條件相符，迄今已獲得的同意將持續有效。

It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR[76]). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces

---

見WP29 05/2014關於「匿名化技術」之意見書（WP216）。

[75] In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.
依GDPR第18條規定，在某些資料運用活動受到限制的情形下，解除限制可能需要當事人的同意。

[76] Recital 171 GDPR states: "Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed."
GDPR前言第171點謂：「本規則取代95/46/EC指令。在本規則施行日前已在進行的運用行為應於本規則生效後兩年內使其符合本規則規定。對於依95/46/EC指令規定以同意為依據的運用行為，如給予同意的方式與本規則規定之要件相符，當事人不必然需要再次給予同意，即可由控管者在本規則施行日後繼續該運用行為。執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效」。

several new requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.[77]
對控管者重要的是，在2018年5月25日前細部審查現行的工作流程與紀錄，以確保現有的同意達到GDPR的標準（見GDPR前言第171點[76]）。在實踐上，GDPR對建置同意機制提高標準，並增設數項新規以要求控管者修改同意機制，而非僅是重新撰寫隱私政策[77]。

For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a "statement or a clear affirmative action", all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent.
舉例來說，由於GDPR要求控管者須可證明獲得有效同意，因此所有未保存參考資訊的推定同意將當然低於GDPR的同意標準，並需要更新。同樣地，因為GDPR要求「聲明或清楚肯定的行動」，因此所有基於當事人以較為暗示之行動（例如預先勾選的選擇同意框格）表達的推定同意，就GDPR的同意標準來說也不恰當。

Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject's wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR's standards, controllers will need to obtain fresh GDPR-compliant consent.
因此，為能證明獲得同意，或能允許更有區別地表達當事人的意思，作業和資訊系統可能需要改版。此外，讓當事人能輕易撤回同意之機制必須存在，且須提供如何撤回同意之資訊。如果現有之獲得與管理同意的程序不符合GDPR標準，控管者將需要獲得新的符合GDPR之同意。

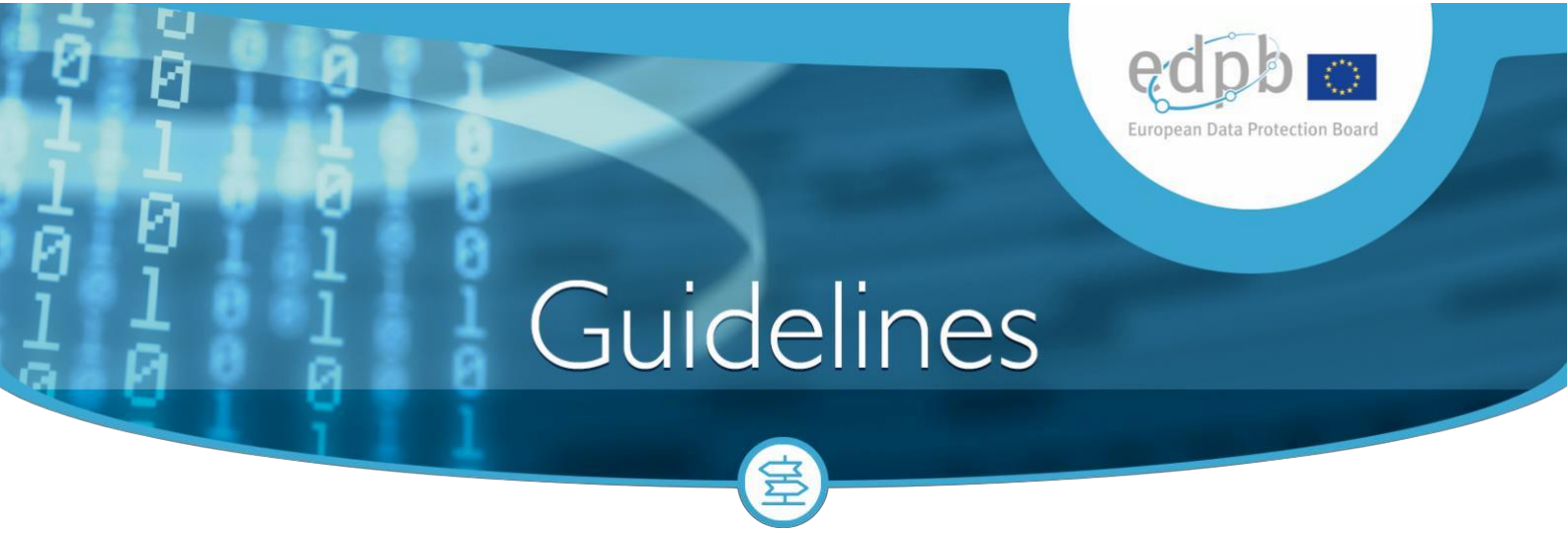
On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.
另一方面，由於知情同意的條件並未要求揭露第13條或第14條的所有要素，GDPR擴增的資訊義務不必然影響在GDPR生效前即已給予之同意的持續有效性（見上方第15頁）（譯註：即本翻譯文件第21頁）。在95/46/EC指令下，並無規範要求將運用之法律依據告知當事人。

If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable –as a one off situation- to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair

[77] As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.
如導言所述，GDPR對於「取得及舉證有效同意」提出更清楚與詳盡的規範。許多新規定是以15/2011關於同意之意見書為依據。

and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing.
如控管者發現，之前在舊法下獲得的同意無法符合GDPR的同意標準時，控管者即應採取行動以遵循該標準，例如以符合GDPR的方式更新同意。在GDPR下，不得在不同合法基礎之間任意變換。如控管者無法以合規方式更新同意，也無法一次性地以不同的資料運用合法基礎轉換至符合GDPR規範，並能同時確保繼續運用符合公平性與課責性時，即應終止該運用行為。在任何情況下，控管者都需要注意合法、公平與透明運用之原則。

-*-*-*-*-*-*-*-*-*-*-*-* END OF DOCUMENT *-*



Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

關於 GDPR（第 3 條）地域範圍之指引 3/2018

Version 2.0

版本 2.0

12 November 2019

2019 年 11 月 12 日

Version history 版本更新歷程

Version 2.0 版本 2.0	12 November 2019 2019 年 11 月 12 日	Adoption of the Guidelines after public consultation 公眾諮詢後通過本指引
Version 1.0 版本 1.0	16 November 2018 2018 年 11 月 16 日	Adoption of the Guidelines for publication consultation 通過本指引供公眾諮詢

Contents 目錄

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing* of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

HAS ADOPTED THE FOLLOWING GUIDELINES:

歐洲個人資料保護委員會

依據歐洲議會與歐盟理事會於 2016 年 4 月 27 日通過歐盟規則 2016/679/EU 第 70 條第 1 項第 e 款，關於運用*個人資料時對自然人之保護與確保該資料之自由流通，以及指令 95/46 / EC 之廢除。

通過以下指引：

*譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而 GDPR 對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將 GDPR 中的 processing 譯為「運用」，processor 譯為「受託運用者」

INTRODUCTION 導言

The territorial scope of General Data Protection Regulation[1] (the GDPR or the Regulation) is determined by Article 3 of the Regulation and represents a significant evolution of the EU data protection law compared to the framework defined by Directive 95/46/EC[2]. In part, the GDPR confirms choices made by the EU legislator and the Court of Justice of the European Union (CJEU) in the context of Directive 95/46/EC. However, important new elements have been introduced. Most importantly, the main objective of Article 4 of the Directive was to define which Member State's national law is applicable, whereas Article 3 of the GDPR defines the territorial scope of a directly applicable text. Moreover, while Article 4 of the Directive made reference to the 'use of equipment' in the Union's territory as a basis for bringing controllers who were "not established on Community territory" within the scope of EU data protection law, such a reference does not appear in Article 3 of the GDPR.

一般資料保護規則（GDPR 或本規則）[1] 第 3 條不只訂定了該規則的地域範圍，也顯示了自歐盟指令 95/46/EU[2] 以來，歐盟在個人資料保護法上的重大進展。某種程度上，GDPR 確認了歐盟立法者以及歐盟法院在指令 95/46/EU 中做出之選擇。然而，GDPR 也引進了重要的新要素。最重要的，指令第 4 條的主要目的是確定成員國的國家法律適用問題，而 GDPR 第 3 條則直接以適用的文字定義了地域範圍。此外，指令第 4 條將「設備的使用」作為「未設立於歐盟境內」之資料控管者適用歐盟個資保護法的依據。然而，此類規範並未出現在 GDPR 第 3 條中。

Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows.

GDPR 第 3 條反映了立法者全面保護位於歐盟境內個資當事人權利之意圖，且在資料保護要件方面，基於全球性的資料傳輸環境，立法者欲為活躍於歐洲市場的公司建立一個公平競爭的環境。

Article 3 of the GDPR defines the territorial scope of the Regulation on the basis of two

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2016年4月27日歐洲議會和理事會在個人資料運用上為保護自然人與確保該資料之自由流通，制定第2016/679號規則（EU），並廢除第95/46 / EC號指令（一般資料保護規則）。

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
1995年10月24日歐洲議會和理事會在個人資料運用上為保護自然人與該資料之自由流通，制定第95/46 / EC號指令。

main criteria: the “establishment” criterion, as per Article 3(1), and the “targeting” criterion as per Article 3(2). Where one of these two criteria is met, the relevant provisions of the GDPR will apply to relevant processing of personal data by the controller or processor concerned. In addition, Article 3(3) confirms the application of the GDPR to the processing where Member State law applies by virtue of public international law.
GDPR 第 3 條根據兩項主要準則定義了該規則的地域範圍：第 3 條第 1 項的「據點」準則以及第 3 條第 2 項的「目標」準則。若資料控管者或資料受託運用者運用個人資料之行為符合前揭任一準則，GDPR 相關規定即適用於該行為。此外，第 3 條第 3 項確認了 GDPR 亦適用於當成員國法律依國際公法可得適用領域內所為之個人資料運用。

Through a common interpretation by data protection authorities in the EU, these guidelines seek to ensure a consistent application of the GDPR when assessing whether particular processing by a controller or a processor falls within the scope of the new EU legal framework. In these guidelines, the EDPB sets out and clarifies the criteria for determining the application of the territorial scope of the GDPR. Such a common interpretation is also essential for controllers and processors, both within and outside the EU, so that they may assess whether they need to comply with the GDPR for a given processing activity.
透過歐盟資料保護機關的統一解釋，在評估資料控管者或資料受託運用者運用個人資料之行為是否屬於新的歐盟法律架構範圍時，這些指引旨在確保 GDPR 適用的一致性。在指引中，歐洲個人資料保護委員會（EDPB）制定並闡明 GDPR 地域範圍適用之標準。位於歐盟內外之資料控管者和受託運用者可藉由這些統一的解釋，評估特定運用活動是否需要遵守 GDPR 的規範。

As controllers or processors not established in the EU but engaging in processing activities falling within Article 3(2) are required to designate a representative in the Union, these guidelines will also provide clarification on the process for the designation of this representative under Article 27 and its responsibilities and obligations.
對非設立於歐盟境內卻符合第 3 條第 2 項涉及資料運用活動之資料控管者或受託運用者，須於歐盟內指定代表。這些指引也將依據第 27 條，闡明指定代表的程序及其責任和義務。

As a general principle, the EDPB asserts that where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing. These guidelines will specify the various scenarios that may arise, depending on the type of processing activities, the entity carrying out these processing activities or the

location of such entities, and will detail the provisions applicable to each situation. It is therefore essential that controllers and processors, especially those offering goods and services at international level, undertake a careful and *in concreto* assessment of their processing activities, in order to determine whether the related processing of personal data falls under the scope of the GDPR.
作為一般原則，EDPB 主張，若個人資料之運用屬於 GDPR 的地域範圍，則此規則的所有規範均適用於該運用。本指引將依據運用活動的類型、執行運用活動的實體或實體之所在地，具體說明可能出現的各種情況，並詳細列舉適用於每種情況之規範。因此，資料控管者和受託運用者，尤其是那些提供國際性商品和服務者，必須對其運用之活動進行詳細且*具體*的評估，以確定相關的個人資料運用是否屬於 GDPR 的適用範圍。

The EDPB underlines that the application of Article 3 aims at determining whether a particular processing activity, rather than a person (legal or natural), falls within the scope of the GDPR. Consequently, certain processing of personal data by a controller or processor might fall within the scope of the Regulation, while other processing of personal data by that same controller or processor might not, depending on the processing activity.
EDPB 強調，第 3 條之適用旨在確認特定之運用活動是否屬於 GDPR 之適用範圍，而非確認當事人（法人或自然人）是否屬於 GDPR 之適用範圍。因此控管者或受託運用者對個人資料之某些運用可能屬於本規則之適用範圍，而由同一控管者或受託運用者對個人資料之其他運用則可能（取決於該運用活動）不屬於本規則之適用範圍。

These guidelines, initially adopted by the EDPB on 16 November, have been submitted to a public consultation from 23rd November 2018 to 18th January 2019 and have been updated taking into account the contributions and feedback received.
本指引最初由 EDPB 於 11 月 16 日通過，在 2018 年 11 月 23 日至 2019 年 1 月 18 日提交公眾諮詢，並於評估獲得之提議和反饋後有所更新。

1. APPLICATION OF THE ESTABLISHMENT CRITERION - ART3(1)

第 3 條第 1 項據點(Establishment)準則之適用

Article 3(1) of the GDPR provides that the "*Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union*

or not."
GDPR 第 3 條第 1 項規定「*本規則適用於資料控管者或受託運用者在歐盟境內設立之據點所為之個人資料運用活動，不論該運用是否發生於歐盟境內*」。

Article 3(1) GDPR makes reference not only to an establishment of a controller, but also to an establishment of a processor. As a result, the processing of personal data by a processor may also be subject to EU law by virtue of the processor having an establishment located within the EU.
GDPR 第 3 條第 1 項不僅適用於資料控管者所設立之據點，亦適用於受託運用者所設立之據點。因此，若受託運用者在歐盟境內設有據點，該受託運用者所為之個人資料運用可能也適用於歐盟之法律。

Article 3(1) ensures that the GDPR applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the Union, regardless of the actual place of the processing. The EDPB therefore recommends a threefold approach in determining whether or not the processing of personal data falls within the scope of the GDPR pursuant to Article 3(1).
第 3 條第 1 項確認 GDPR 適用於資料控管者或受託運用者在歐盟境內設立之據點所為之資料運用活動，不論該運用是否發生於歐盟境內。因此，EDPB 建議一種三重判斷法來決定個人資料之運用是否屬於 GDPR 第 3 條第 1 項之適用範圍

The following sections clarify the application of the establishment criterion, first by considering the definition of an 'establishment' in the EU within the meaning of EU data protection law, second by looking at what is meant by 'processing in the context of the activities of an establishment in the Union', and lastly by confirming that the GDPR will apply regardless of whether the processing carried out in the context of the activities of this establishment takes place in the Union or not.
以下篇章將闡釋據點準則之適用。第一部分考量在歐盟資料保護法下，於歐盟境內設立「據點」之定義。第二部分著眼於「在歐盟境內之據點，於其活動範圍內所為的資料運用」之定義。最後一部分則確認無論該據點於其活動範圍內所為之運用是否發生於歐盟境內，GDPR 仍適用之。

a) "An establishment in the Union"
「歐盟境內之據點」

Before considering what is meant by "an establishment in the Union" it is first necessary to identify who is the controller or processor for a given processing activity.

According to the definition in Article 4(7) of the GDPR, controller means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". A processor, according to Article 4(8) of the GDPR, is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". As established by relevant CJEU case law and previous WP29 opinion[3], the determination of whether an entity is a controller or processor for the purposes of EU data protection law is a key element in the assessment of the application of the GDPR to the personal data processing in question.

在考量「歐盟境內之據點」的含義前，第一必須先確認誰是資料運用行為的控管者或受託運用者。依據 GDPR 第 4 條第 7 項，控管者係指「單獨或與他人共同決定個人資料運用之目的及方式之自然人或法人、公務機關、局處或其他機構」。依據 GDPR 第 4 條第 8 款，受託運用者係指「代表資料控管者運用個人資料之自然人或法人、公務機關、局處或其他機構」。依據歐盟法院相關之判例法及先前 29 條工作小組（WP29[3]）意見，決定某實體是否屬於歐盟個人資料保護法下之控管者或受託運用者，是檢視 GDPR 是否適用於個人資料運用行為的關鍵要素。

While the notion of "main establishment" is defined in Article 4(16), the GDPR does not provide a definition of "establishment" for the purpose of Article 3[4]. However, Recital 22[5] clarifies that an "*[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.*"

雖然第 4 條第 16 款對「主要據點」(main establishment) 的概念做了解釋，但 GDPR 並沒有針對第 3 條的「據點」提供定義[4]。然而，前言第 22 點[5]闡明「*據點係指透過穩定安排，從事於有效及實際的活動。安排之法律形式，不因其係透過分公司*

[3] G29 WP169 - Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16th February 2010 and under revision by the EDPB

G29WP169 – 意見1/2010 定義「控管者」與「受託運用者」，於2010年2月16日通過，並由EDPB進行修訂。

[4] The definition of "main establishment" is mainly relevant for the purpose of determining the competence of the supervisory authorities concerned according to Article 56 GDPR. See the WP29 Guidelines for identifying a controller or processor's lead supervisory authority (16/EN WP 244 rev.01) – endorsed by the EDPB.

「主要據點」之定義大體上是和決定GDPR第56條監管機關之權限有關。請參閱WP29確認控管者或受託運用者之主責監管機關指引（16 / EN WP 244 更新版本0.1）- 由EDPB採認。

[5] Recital 22 of the GDPR: "Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

GDPR前言第22點: 「控管者或受託運用者在歐盟境內之據點所為之一切個人資料運用均應受本規則之拘束，無論其運用行為本身是否發生於歐盟境內。據點係指透過穩定安排，從事於有效及實際之活動。此等安排之法律型式，不因其係透過分公司或具有法人資格之子公司所為而有所不同。」

或具有法人資格之子公司所為而有不同」。

This wording is identical to that found in Recital 19 of Directive 95/46/EC, to which reference has been made in several CJEU rulings broadening the interpretation of the term "establishment", departing from a formalistic approach whereby undertakings are established solely in the place where they are registered[6]. Indeed, the CJEU ruled that the notion of establishment extends to any real and effective activity — even a minimal one — exercised through stable arrangements[7]. In order to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet[8].
此一措辭與 95/46/EU 指令中前言第 19 點相同。前言第 19 點已被數個歐盟法院案例引用，並擴充了對「據點」一詞的解釋，不局限在形式上的觀點，也就是據點之設立不應限縮在其所註冊之地點 [6]。事實上，歐盟法院裁定，「據點」之範疇應延伸至經由穩定的安排，而從事任何實質且有效的活動，即使是一個最小量的活動[7]。為決定歐盟外之實體是否於某一成員國境內設有據點，必須根據其經濟行為的具體性質以及所提供之服務，來考量在該成員國內活動安排的穩定程度及活動的有效執行。此對僅透過網路提供服務的企業主體尤其如是[8]。

The threshold for "stable arrangement[9]" can actually be quite low when the centre of activities of a controller concerns the provision of services online. As a result, in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement (amounting to an 'establishment' for the purposes of Art 3(1)) if that employee or agent acts with a sufficient degree of stability. Conversely, when an employee is based in the EU but the processing is not being carried out in the context of the activities of the EU-based employee in the Union (i.e. the processing relates to activities of the controller outside the EU), the mere presence of an employee in the EU will not result in that processing falling within the scope of

[6] See in particular Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12), Weltimmo v NAIH (C- 230/14), Verein für Konsumenteninformation v Amazon EU (C-191/15) and Wirtschaftsakademie Schleswig- Holstein (C-210/16).
特別參閱Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12), Weltimmo v NAIH (C- 230/14), Verein für Konsumenteninformation v Amazon EU (C-191/15) 以及 Wirtschaftsakademie Schleswig- Holstein (C-210/16)。
[7] Weltimmo, paragraph 31.
Weltimmo v NAIH (C- 230/14)，第31段。
[8] Weltimmo, paragraph 29.
Weltimmo v NAIH (C- 230/14)，第29段。
[9] Weltimmo, paragraph 31.
Weltimmo v NAIH (C- 230/14)，第31段。

the GDPR. In other words, the mere presence of an employee in the EU is not as such sufficient to trigger the application of the GDPR, since for the processing in question to fall within the scope of the GDPR, it must also be carried out in the context of the activities of the EU-based employee.

「穩定安排」[9]的門檻，對以提供網路服務為其活動中心的控管者來說，實際上是相當低的。因此，在某些情況下，一個非設立於歐盟的實體，只要其僱員或代理人在歐盟境內之行為具有足夠的穩定性，即使只有一個僱員或代理人，也可能足以符合穩定安排（依據第 3 條第 1 項得認作為「據點」）之要件。相反的，若某個僱員位於歐盟境內，但運用之執行並非屬位於歐盟境內僱員之活動範圍內（即該運用涉及位於歐盟外控管者之活動時），則僅於歐盟境內存在該名僱員之情況，不會導致該運用屬於 GDPR 之適用範圍。易言之，僅於歐盟境內存在一名僱員並不足以觸發 GDPR 之適用，因為要使相關運用落入 GDPR 之範圍，該運用必須屬於位於歐盟境內僱員之活動範圍內。

The fact that the non-EU entity responsible for the data processing does not have a branch or subsidiary in a Member State does not preclude it from having an establishment there within the meaning of EU data protection law. Although the notion of establishment is broad, it is not without limits. It is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking's website is accessible in the Union[10].

在歐盟個人資料保護法的定義中，負責資料運用的非位於歐盟之實體，於歐盟成員國內未設有分公司或子公司之事實，並不排除其在成員國內設立「據點」之可能。雖然據點的涵蓋範圍較廣，但並非沒有限制。不得僅因某一事業網站可於歐盟境內瀏覽，即認定該非位於歐盟境內之實體於歐盟境內設有據點[10]。

Example 1: A car manufacturing company with headquarters in the US has a fully-owned branch and office located in Brussels overseeing all its operations in Europe, including marketing and advertisement.

示例 1：一家總部位於美國的汽車製造公司，在布魯塞爾設有一家全資分公司及辦公室，負責監督歐洲業務，包括行銷和廣告。

The Belgian branch can be considered to be a stable arrangement, which exercises real and effective activities in light of the nature of the economic activity carried out by the car manufacturing company. As such, the Belgian branch could therefore be considered as an establishment in the Union, within the meaning of the GDPR.

[10] CJEU, Verein für Konsumenteninformation v. Amazon EU Sarl, Case C 191/15, 28 July 2016, paragraph 76 (hereafter "Verein für Konsumenteninformation").
歐盟法院， Verein für Konsumenteninformation v. Amazon EU Sarl, Case C 191/15，2016年7月28日，第76段。

位於比利時的分公司可被視為是一個穩定安排，該分公司是根據汽車製造公司所執行經濟活動之性質，進行實際且有效的活動。因此，在 GDPR 定義中，比利時的分公司可被認定為係設立於歐盟境內之據點。

Once it is concluded that a controller or processor is established in the EU, an *in concreto* analysis should then follow to determine whether the processing in question is carried out in the context of the activities of this establishment, in order to determine whether Article 3(1) applies. If a controller or processor established outside the Union exercises "a real and effective activity - even a minimal one" - through "stable arrangements", regardless of its legal form (e.g. subsidiary, branch, office...), in the territory of a Member State, this controller or processor can be considered to have an establishment in that Member State[11]. It is therefore important to consider whether the processing of personal data takes place "in the context of the activities of" such an establishment as highlighted in Recital 22.

為確認第 3 條第 1 項之適用，一旦控管者或受託運用者被認定於歐盟境內設有據點，即應採用*具體*的分析方式 (*in concreto*) 來決定，系爭資料運用是否是屬於該據點活動範圍內之行為。若設立於歐盟外之控管者或受託運用者，經由「穩定安排」，無論其法律形式（例如子公司、分公司或辦公室），在成員國的領土範圍內，實行實際且有效之活動（即使是最小限度之活動），即可被認為於該成員國內設有據點[11]。因此，如前言第 22 點中所強調，資料運用行為是否屬於該據點「活動範圍內之行為」是很重要的考量。

b) Processing of personal data carried out "in the context of the activities of" an establishment

b) 個人資料之運用屬於據點「活動範圍內」之行為

Article 3(1) confirms that it is not necessary that the processing in question is carried out "by" the relevant EU establishment itself; the controller or processor will be subject to obligations under the GDPR whenever the processing is carried out "in the context of the activities" of its relevant establishment in the Union. The EDPB recommends that determining whether processing is being carried out in the context of an establishment of the controller or processor in the Union for the purposes of Article 3(1) should be carried out on a case-by-case basis and based on an analysis *in concreto*. Each scenario

[11] See in particular para 29 of the Weltimmo judgment, which emphasizes a flexible definition of the concept of 'establishment' and clarifies that 'the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.'
特別參閱Weltimmo判決第29段，其中強調對「據點」概念的彈性定義，並闡明「安排的穩定程度和有效地執行活動，必須根據該經濟活動的具體性質以及所提供之服務，做進一步解釋」。

must be assessed on its own merits, taking into account the specific facts of the case.
依據第 3 條第 1 項，資料運用並非必須由位於歐盟境內之據點執行，只要運用行為係屬於該相關位於歐盟境內據點的活動範圍內，資料控管者或受託運用者即會受到 GDPR 義務之約束。EDPB 建議，鑒於第 3 條第 1 項之目的，決定運用是否屬於控管者或受託運用者據點活動範圍內之行為，應依據個案研究 (case-by-case)，並依循*具體*的方式分析。任一案件都需考量其特殊具體事實，並根據自身的特性進行評估。

The EDPB considers that, for the purpose of Article 3(1), the meaning of "*processing in the context of the activities of an establishment of a controller or processor*" is to be understood in light of the relevant case law. On the one hand, with a view to fulfilling the objective of ensuring effective and complete protection, the meaning of "in the context of the activities of an establishment" cannot be interpreted restrictively[12]. On the other hand, the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law. Some commercial activity carried out by a non-EU entity within a Member State may indeed be so far removed from the processing of personal data by this entity that the existence of the commercial activity in the EU would not be sufficient to bring that data processing by the non-EU entity within the scope of EU data protection law[13].
EDPB 認為，就第 3 條第 1 項之目的而言，應根據相關判例法來解釋何謂「*資料控管者或受託運用者所設據點活動範圍內所為之資料運用*」。一方面，為達到有效且完整保護之目的，「據點活動範圍」之含義不應被限縮解釋[12]。另一方面，在 GDPR 中，據點的存在也不應過寬解釋，以致於任何存在於歐盟的實體，即使與非位於歐盟實體之資料運用活動，僅有最遠端的連結，亦會被認為其活動屬於歐盟個人資料保護法的適用範圍。當由非設立於歐盟的實體於成員國內所為之商業活動，與運用個人資料行為大相徑庭時，於此非歐盟實體位於歐盟境內之商業活動則不足以使該運用個人資料的行為適用歐盟個資保護法[13]。

Consideration of the following two factors may help to determine whether the processing is being carried out by a controller or processor in the context of its establishment in the Union.

---

[12] Weltimmo, paragraph 25 and Google Spain, paragraph 53.
Weltimmo v NAIH (C- 230/14)，第25段和Google Spain第53段。
[13] WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16th December 2015.
WP 179更新 - 根據2015年12月16日歐盟法院對Google Spain判決於相關適用法律更新意見8/2010。

就下列兩項因素之考量，可協助確認運用是否屬於控管者或受託運用者位於歐盟境內據點活動範圍內之行為：

i) *Relationship between a data controller or processor outside the Union and its local establishment in the Union*

i) *設立於歐盟外之資料控管者或受託運用者與其歐盟本地據點之關聯*

The data processing activities of a data controller or processor established outside the EU may be inextricably linked to the activities of a local establishment in a Member State, and thereby may trigger the applicability of EU law, even if that local establishment is not actually taking any role in the data processing itself[14]. If a case by case analysis on the facts shows that there is an inextricable link between the processing of personal data carried out by a non-EU controller or processor and the activities of an EU establishment, EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data[15].

當設立於歐盟境外資料控管者或受託運用者之資料運用活動，與設立於成員國境內當地據點的活動密不可分時，即使歐盟本地據點並未實際參與任何資料運用，亦可觸發歐盟法律的適用[14]。若於個案分析中，事實證明設立於歐盟外之控管者或受託運用者的個人資料運用行為與設立於歐盟內之據點的活動，存在著不可分割之關聯，歐盟法律將適用於歐盟外實體所為之資料運用行為，無論於歐盟內之據點是否參與此資料之運用[15]。

ii) *Revenue raising in the Union*

ii) *歐盟境內收益之增加*

Revenue-raising in the EU by a local establishment, to the extent that such activities can be considered as "inextricably linked" to the processing of personal data taking place outside the EU and individuals in the EU, may be indicative of processing by a non-EU controller or processor being carried out "in the context of the activities of the EU establishment", and may be sufficient to result in the application of EU law to such processing[16].

---

[14] CJEU, Google Spain, Case C 131/12.
歐盟法院，Google Spain, Case C 131/12。

[15] G29WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16th December 2015.
G29WP 179更新 - 根據2015年12月16日歐盟法院對Google Spain判決於相關適用法律更新意見8/2010。

[16] This may potentially be the case, for example, for any foreign operator with a sales office or some other presence in the EU, even if that office has no role in the actual data processing, in particular where the processing takes place in the context of the sales activity in the EU and the activities of the

當設立於歐盟境內之據點收益的增加，與設立於歐盟外之資料控管者或受託運用者對歐盟內個人所為之資料運用行為被視為「密不可分」時，該運用行為即可認作係非設立於歐盟之資料控管者或受託運用者，在歐盟境內所設據點的活動範圍內，所為之資料運用行為，並足以引發歐盟法律之適用[16]。

The EDPB recommends that non-EU organisations undertake an assessment of their processing activities, first by determining whether personal data are being processed, and secondly by identifying potential links between the activity for which the data is being processed and the activities of any presence of the organisation in the Union. If such a link is identified, the nature of this link will be key in determining whether the GDPR applies to the processing in question, and must be assessed inter alia against the two elements listed above.

EDPB 建議非設立於歐盟之企業需評估自身資料運用行為。首先須確認是否有運用個人資料之情事，其次是確認資料運用活動與企業設立於歐盟境內之任何組織的活動，是否存在可能的關聯性。若可確認其關聯性，該關聯之性質，將會是決定 GDPR 適用的關鍵要素，因此，除其他事項外，必須基於上述兩項要件進行評估。

Example 2: An e-commerce website is operated by a company based in China. The personal data processing activates of the company are exclusively carried out in China. The Chinese company has established a European office in Berlin in order to lead and implement commercial prospection and marketing campaigns towards EU markets.

示例 2: 某電子商務網站由一設立於中國的公司經營。該公司個人資料運用之活動僅限於中國境內。為了領導及執行針對歐洲市場的商業勘查和銷售活動，該公司於柏林設立了一間歐洲辦事處。

In this case, it can be considered that the activities of the European office in Berlin are inextricably linked to the processing of personal data carried out by the Chinese e-commerce website, insofar as the commercial prospection and marketing campaign towards EU markets notably serve to make the service offered by the e-commerce website profitable. The processing of personal data by the Chinese company in relation to EU sales is indeed inextricably linked to the activities of the European office in Berlin relating to commercial prospection and marketing campaign towards EU market. The processing of personal data by the Chinese company in connection with EU sales can therefore be considered as carried out in the context of the activities of the European

---

establishment are aimed at the inhabitants of the Member States in which the establishment is located (WP179 update).

此類型可能發生之情況如，任何在歐盟設有銷售辦事處或其他態樣的外國運營商，即使該辦事處沒有參與任何實際資料運用行為，尤其當資料運用行為與歐盟銷售活動相關，而辦事處主要業務是針對成員國當地居民的情形（WP179更新）。

office, as an establishment in the Union. This processing activity by the Chinese company will therefore be subject to the provisions of the GDPR as per its Article 3(1).
在此案例中，若針對歐洲市場的商業勘查和行銷活動是為了使電子商務網站所提供之服務獲利，柏林歐洲辦事處之活動即可被視為與中國電子商務網站所執行之個人資料運用行為有著密不可分之關聯。中國公司就歐盟銷售所為之個人資料運用，的確與位於柏林的歐洲辦事處針對歐洲市場的商業勘查和銷售所為之活動密不可分。因此，中國公司就歐盟銷售所為之個人資料運用行為，可被視作為歐盟辦事處(位於歐盟境內之據點)活動範圍內之行為。依據第 3 條第 1 項，該中國公司之運用活動將因此屬於 GDPR 之適用範圍。

Example 3: A hotel and resort chain in South Africa offers package deals through its website, available in English, German, French and Spanish. The company does not have any office, representation or stable arrangement in the EU.
示例 3：位於南非的一家酒店和度假村連鎖店，透過網站提供套裝優惠。該網站提供英文、德文、法文以及西班牙文的版本。該公司於歐盟境內未設置任何辦事處、代表處或其他穩定安排。

In this case, in the absence of any representation or stable arrangement of the hotel and resort chain within the territory of the Union, it appears that no entity linked to this data controller in South Africa can qualify as an establishment in the EU within the meaning of the GDPR. Therefore the processing at stake cannot be subject to the provisions of the GDPR, as per Article 3(1).
在此案例中，因於歐盟境內未設立任何酒店或度假村連鎖店的代表處或穩定安排，在 GDPR 的定義下，沒有任何實體可被視為是此南非資料控管者設立於歐盟境內之據點。因此，該資料運用行為不屬於 GDPR 第 3 條第 1 項的適用範圍。

However, it must be analysed *in concreto* whether the processing carried out by this data controller established outside the EU can be subject to the GDPR, as per Article 3(2).
然而，仍必須依據*具體*的分析方式，確認非設立於歐盟境內之控管者所為之資料運用行為，是否屬於 GDPR 第 3 條第 2 項的適用範圍。

c) Application of the GDPR to the establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not
c) GDPR 適用於控管者或受託運用者在歐盟境內設立之據點，不論資料運用是否發生於歐盟境內

As per Article 3(1), the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union triggers the application of the GDPR and the related obligations for the data controller or processor concerned.
依據第 3 條第 1 項，任何控管者或受託運用者在歐盟據點活動範圍內所為之資料運用行為，皆可引發 GDPR 及其對資料控管者或受託運用者相關義務規範之適用。

The text of the GDPR specifies that the Regulation applies to processing in the context of the activities of an establishment in the EU "*regardless of whether the processing takes place in the Union or not*". It is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.
GDPR 的本文明定，本規則適用於設立於歐盟境內之據點所為之個人資料運用活動，「*不論該運用是否發生於歐盟境內*」。當資料控管者或受託運用者，經由以設置據點之方式，於歐盟內存在，且資料之運用屬於該據點活動範圍內之事實，即有 GDPR 對此運用活動之適用性。因此，運用行為之地點，與歐盟境內據點活動範圍內所為之運用是否適用 GDPR 無關。

Example 4: A French company has developed a car-sharing application exclusively addressed to customers in Morocco, Algeria and Tunisia. The service is only available in those three countries but all personal data processing activities are carried out by the data controller in France.
示例 4：一間法國公司，開發了一個專門針對摩洛哥、阿爾及利亞和突尼西亞客戶的乘車共享應用程式。該服務僅提供於此三個國家，但所有個人資料運用活動均由位於法國的資料控管者執行。

While the collection of personal data takes place in non-EU countries, the subsequent processing of personal data in this case is carried out in the context of the activities of an establishment of a data controller in the Union. Therefore, even though processing relates to personal data of data subjects who are not in the Union, the provisions of the GDPR will apply to the processing carried out by the French company, as per Article 3(1).
在此案例中，雖然個人資料的蒐集發生在非歐盟國家，但資料的後續運用，皆由資料控管者設立於歐盟境內之據點執行。因此，即使資料運用所涉及之當事人非位於歐盟境內，依據第 3 條第 1 項之規定，GDPR 的規則仍適用於該法國公司運

用個人資料之行為。

Example 5: A pharmaceutical company with headquarters in Stockholm has located all its personal data processing activities with regards to its clinical trial data in its branch based in Singapore. In this case, while the processing activities are taking place in Singapore, that processing is carried out in the context of the activities of the pharmaceutical company in Stockholm, i.e. of a data controller established in the Union. The provisions of the GDPR therefore apply to such processing, as per Article 3(1).

示例 5：一間總部設立於斯德哥爾摩的製藥公司，其所有與臨床試驗相關之個人資料運用活動皆係由位於新加坡的分公司執行。於此情況下，雖然所有運用活動皆發生於新加坡，該運用之執行應屬位於斯德哥爾摩製藥公司之活動範圍內，意即，屬於設立於歐盟境內之資料控管者之活動範圍內。依據第 3 條第 1 項之規定，GDPR 之規則仍適用於該運用。

In determining the territorial scope of the GDPR, geographical location will be important under Article 3(1) with regard to the place of establishment of:
依據第 3 條第 1 項，在確認 GDPR 的地域範圍時，據點設立之地理位置於以下兩種情形至關重要：
- the controller or processor itself (is it established inside or outside the Union?);
- 控管者或受託運用者本身的地理位置（設立於歐盟境內或境外？）
- any business presence of a non-EU controller or processor (does it have an establishment in the Union?)
- 非設立於歐盟境內之控管者或受託運用者任何業務存在地點（是否在歐盟境內設有據點？）

However, geographical location is not important for the purposes of Article 3(1) with regard to the place in which processing is carried out, or with regard to the location of the data subjects in question.
然而，就第 3 條第 1 項之目的，地理位置對資料運用地點以及當事人所在地而言，並不重要。

The text of Article 3(1) does not restrict the application of the GDPR to the processing of personal data of individuals who are in the Union. The EDPB therefore considers that any personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being

processed. This approach is supported by Recital 14 of the GDPR which states that "*[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.*"

第 3 條第 1 項條文本身並未限縮 GDPR 的適用範圍在運用位於歐盟境內之自然人的個人資料。因此，EDPB 認為，無論當事人的位置或國籍如何，任何個人資料運用行為，只要屬於資料控管者或受託運用者在歐盟境內所設據點的活動範圍內，皆屬於 GDPR 的適用範圍。GDPR 的前言第 14 點也支持此見解：「*本規則所保護者應適用於自然人，不論當事人之國籍或住居所，凡涉及其個人資料之運用均屬之*」。

d) Application of the establishment criterion to controller and processor
d)資料控管者和受託運用者設置據點準則之適用

As far as processing activities falling under the scope of Article 3(1) are concerned, the EDPB considers that such provisions apply to controllers and processors whose processing activities are carried out in the context of the activities of their respective establishment in the EU. While acknowledging that the requirements for establishing the relationship between a controller and a processor[17] does not vary depending on the geographical location of the establishment of a controller or processor, the EDPB takes the view that when it comes to the identification of the different obligations triggered by the applicability of the GDPR as per Article 3(1), the processing by each entity must be considered separately.

EDPB 認為，只要資料運用活動屬於第 3 條第 1 項之適用範圍，即運用行為屬於設立於歐盟境內各自據點的活動範圍內，該條款則適用於資料控管者和受託運用者。雖然認知到資料控管者和受託運用者之間建立連結關係的要求不會因控管者和受託運用者設置的地理位置而有所不同[17]，EDPB 認為，依據第 3 條第 1 項，在確認因 GDPR 的適用性而引發不同的義務時，每個實體的資料運用行為皆必須單獨考量。

The GDPR envisages different and dedicated provisions or obligations applying to data controllers and processors, and as such, should a data controller or processor be subject

[17] In accordance with Article 28, the EDPB recalls that processing activities by a processor on behalf of a controller shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller, and that controllers shall only use processors providing sufficient guarantees to implement appropriate measures in such manner that processing will meet the requirement of the GDPR and ensure the protection of data subjects' rights.
根據第28條，EDPB回顧當運用行為係由受託運用者代表控管者所為時，該運用需受到歐盟或其成員國法律中有關契約或其他立法之管制，該等規定對受託運用者及控管者具有拘束力。控管者得任用之受託運用者，需能提供充足保證會施以適當且符合GDPR要求之措施，並確保個資當事人權利之保障。

to the GDPR as per Article 3(1), the related obligations would apply to them respectively and separately. In this context, the EDPB notably deems that a processor in the EU should not be considered to be an establishment of a data controller within the meaning of Article 3(1) merely by virtue of its status as processor on behalf of a controller.
GDPR 對資料控管者和受託運用者設計了不同且專用的條款或義務。因此，若資料控管者或受託運用者依第 3 條第 1 項受拘束於 GDPR 時，相關義務將分別適用之。於此情形，EDPB 認為，位於歐盟的資料受託運用者不應僅憑其代表控管者而作為受託運用者的地位，而被視為屬於第 3 條第 1 項定義上資料控管者所設立之據點。

The existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both, should one of these two entities not be established in the Union.
若控管者或受託運用者其中之一非位於歐盟境內，二者間存在的關聯性不一定會觸發 GDPR 同時適用於控管者與受託運用者。

An organisation processing personal data on behalf of, and on instructions from, another organisation (the client company) will be acting as processor for the client company (the controller). Where a processor is established in the Union, it will be required to comply with the obligations imposed on processors by the GDPR (the 'GDPR processor obligations'). If the controller instructing the processor is also located in the Union, that controller will be required to comply with the obligations imposed on controllers by the GDPR (the 'GDPR controller obligations'). Processing activity which, when carried out by a controller, falls within the scope of the GDPR by virtue of Art 3(1) will not fall outside the scope of the Regulation simply because the controller instructs a processor not established in the Union to carry out that processing on its behalf.
當一間組織代表另一間組織（客戶公司）並依其指示進行資料運用行為，前者即為後者（資料控管者）之資料受託運用者。若受託運用者設立於歐盟境內，則須遵守 GDPR 對受託運用者訂定之相關義務（GDPR 受託運用者義務）。若控管者亦位於歐盟境內，該控管者必須遵守 GDPR 對控管者訂定之相關義務（GDPR 控管者義務）。當運用活動係由控管者執行，且依據第 3 條第 1 項屬於 GDPR 之適用範圍時，不會僅因控管者指示非設立於歐盟境內之受託運用者代表其執行該運用，而使該運用不受本規則拘束。

i) Processing by a controller established in the EU instructing a processor not established in the Union
i) 位於歐盟境內之控管者任用非設立於歐盟境內之受託運用者

Where a controller subject to GDPR chooses to use a processor located outside the Union for a given processing activity, it will still be necessary for the controller to ensure by contract or other legal act that the processor processes the data in accordance with the GDPR. Article 28(3) provides that the processing by a processor shall be governed by a contract or other legal act. The controller will therefore need to ensure that it puts in place a contract with the processor addressing all the requirements set out in Article 28(3). In addition, it is likely that, in order to ensure that it has complied with its obligations under Article 28(1) – to use only a processor providing sufficient guarantees to implement measures in such a manner that processing will meet the requirements of the Regulation and protect the rights of data subjects – the controller may need to consider imposing, by contract, the obligations placed by the GDPR on processors subject to it. That is to say, the controller would have to ensure that the processor not subject to the GDPR complies with the obligations, governed by a contract or other legal act under Union or Member State law, referred to Article 28(3).
當適用於 GDPR 之控管者就特定運用活動，任用位於歐盟外之受託運用者時，該控管者仍須確保藉由契約或其他立法之拘束，使受託運用者運用個人資料之行為符合 GDPR 的規範。第 28 條第 3 項規定，受託運用者所為運用行為應受契約或其他立法之拘束。控管者因此需確保和受託運用者之契約滿足第 28 條第 3 項所有要件。此外，第 28 條第 1 項規定控管者僅得任用可提供充足保證會實施適當措施、使運用行為符合本規則要求，並確保當事人權利保障之受託運用者。為確保遵守該條之義務，控管者可能需要考量透過契約強加 GDPR 之義務於受託運用者。也就是說，依據第 28 條第 3 項，控管者須藉由契約或歐盟法或成員國法之其他立法拘束，使不受 GDPR 約束之受託運用者履行其相關義務。

The processor located outside the Union will therefore become indirectly subject to some obligations imposed by controllers subject to the GDPR by virtue of contractual arrangements under Article 28. Moreover, provisions of Chapter V of the GDPR may apply.
因此，藉由第 28 條之契約安排，屬於 GDPR 適用範圍之控管者可強加某些義務於位於歐盟外之受託運用者，使其間接受到 GDPR 之管轄。此外，GDPR 第 5 章的規定亦有適用之可能。

Example 6: A Finnish research institute conducts research regarding the Sami people. The institute launches a project that only concerns Sami people in Russia. For this project the institute uses a processor based in Canada.
示例 6：一家芬蘭研究機構對薩米人進行研究，且研究項目僅涉及俄羅斯的薩米人。該研究機構任用位於加拿大的資料受託運用者。

The Finnish controller has a duty to only use processors that provide sufficient guarantees to implement appropriate measures in such manner that processing will meet the requirement of the GDPR and ensure the protection of data subjects' rights. The Finnish controller needs to enter into a data processing agreement with the Canadian processor, and the processor's duties will be stipulated in that legal act.
位於芬蘭的控管者有責任確保任用可提供充足保證會實施適當措施、使運用行為符合 GDPR 要求，並確保當事人權利保障之受託運用者。芬蘭的控管者需與加拿大的受託運用者簽訂資料運用契約，並在這法律行為中訂定受託運用者之相關義務。

ii) *Processing in the context of the activities of an establishment of a processor in the Union*
ii) *資料運用行為屬於受託運用者位於歐盟境內據點之活動範圍內*

Whilst case law provides us with a clear understanding of the effect of processing being carried out in the context of the activities of an EU establishment of the controller, the effect of processing being carried out in the context of the activities of an EU establishment of a processor is less clear.
雖然判決先例對控管者位於歐盟境內據點所為資料運用行為之影響提供清楚的說明，但對受託運用者位於歐盟境內據點所為資料運用行為之影響為何，則較不清楚。

The EDPB emphasises that it is important to consider the establishment of the controller and processor separately when determining whether each party is of itself 'established in the Union'.
EDPB 強調，當在確認是否雙方皆各自「設立於歐盟境內」時，控管者和受託運用者所設立之據點必需分別考量。

The first question is whether the controller itself has an establishment in the Union, and is processing in the context of the activities of that establishment. Assuming the controller is not considered to be processing in the context of its own establishment in the Union, that controller will not be subject to GDPR controller obligations by virtue of Article 3(1) (although it may still be caught by Article 3(2)). Unless other factors are at play, the processor's EU establishment will not be considered to be an establishment in respect of the controller.
第一個須考量的問題在於控管者是否在歐盟境內設有據點且資料運用行為是否屬於該據點的活動範圍內。假設控管者的運用行為不被認為屬於歐盟所設據點的活

動範圍內，依據第 3 條第 1 項之規定，該控管者將不受 GDPR 之拘束（雖然仍有第 3 條第 2 項適用之可能）。除非有其他因素，受託運用者設立於歐盟境內之據點將不會被視為係與控管者相關之據點。

The separate question then arises of whether the processor is processing in the context of its establishment in the Union. If so, the processor will be subject to GDPR processor obligations under Article 3(1). However, this does not cause the non-EU controller to become subject to the GDPR controller obligations. That is to say, a "non-EU" controller (as described above) will not become subject to the GDPR simply because it chooses to use a processor in the Union.
另一個須考量的問題在於受託運用者所為之運用行為是否屬於其設立於歐盟境內據點的活動範圍內。如果是，依據第 3 條第 1 項，受託運用者將受 GDPR 受託運用者義務所拘束。然而，這並不會導致非設立於歐盟境內之控管者受到 GDPR 控管者義務之拘束。如前所述，「非位於歐盟境內」之控管者，不會僅因任用位於歐盟境內之受託運用者，而受 GDPR 拘束。

By instructing a processor in the Union, the controller not subject to GDPR is not carrying out processing "in the context of the activities of the processor in the Union". The processing is carried out in the context of the controller's own activities; the processor is merely providing a processing service[18] which is not "inextricably linked" to the activities of the controller. As stated above, in the case of a data processor established in the Union and carrying out processing on behalf of a data controller established outside the Union and not subject to the GDPR as per Article 3(2), the EDPB considers that the processing activities of the data controller would not be deemed as falling under the territorial scope of the GDPR merely because it is processed on its behalf by a processor established in the Union. However, even though the data controller is not established in the Union and is not subject to the provisions of the GDPR as per Article 3(2), the data processor, as it is established in the Union, will be subject to the relevant provisions of the GDPR as per Article 3(1).
即使任用位於歐盟境內之受託運用者，不受 GDPR 約束之控管者，其運用行為仍不屬於位於歐盟境內之受託運用者活動範圍內所為之運用行為。該運用行為係由控管者在其自身活動範圍內所實行，而受託運用者僅提供運用服務 [18]，該服務與控管者的活動並非「密不可分」。如上所述，EDPB 認為，位於歐盟境內之資料受託運用者，代表非設立於歐盟且不屬於 GDPR 第 3 條第 2 項管轄範圍內之資料控管者執行資料運用時，該控管者之運用活動不會僅因為任用位於歐盟境內之受託運用者代表其執行，而被視為屬於 GDPR 的地域範圍。然而，即使資料控管者非

[18] The offering of a processing service in this context cannot be considered either as an offer of a service to data subjects in the Union.
此處所提及之運用服務不得係為歐盟境內個資當事人所提供之服務。

設立於歐盟境內且不屬於 GDPR 第 3 條第 2 項適用範圍，設立於歐盟境內之資料受託運用者，仍應根據第 3 條第 1 項，受 GDPR 的相關規範約束。

Example 7: A Mexican retail company enters into a contract with a processor established in Spain for the processing of personal data relating to the Mexican company's clients. The Mexican company offers and directs its services exclusively to the Mexican market and its processing concerns exclusively data subjects located outside the Union.
示例 7：一間墨西哥零售公司與一個位於西班牙的受託運用者簽訂契約，以運用與墨西哥公司客戶相關之個人資料。該墨西哥公司僅對墨西哥市場提供服務，且運用行為僅涉及歐盟外之當事人。

In this case, the Mexican retail company does not target persons on the territory of the Union through the offering of goods or services, nor it does monitor the behaviour of person on the territory of the Union. The processing by the data controller, established outside the Union, is therefore not subject to the GDPR as per Article 3(2).
在此案例中，墨西哥零售公司不僅沒有針對歐盟境內之個人提供商品或服務，亦無監控歐盟境內個人之行為。因此，設立於歐盟外之資料控管者所為的運用行為，不受 GDPR 第 3 條第 2 項之拘束。

The provisions of the GDPR do not apply to the data controller by virtue of Article 3(1) as it is not processing personal data in the context of the activities of an establishment in the Union. The data processor is established in Spain and therefore its processing will fall within the scope of the GDPR by virtue of Article 3(1). The processor will be required to comply with the processor obligations imposed by the regulation for any processing carried out in the context of tis activities.
依據第 3 條第 1 項，GDPR 之規定不適用於該資料控管者，因其所為之運用並不屬於位於歐盟境內據點活動範圍內所為之運用。資料受託運用者位於西班牙，因此依據第 3 條第 1 項，其所為之運用將屬於 GDPR 之適用範圍。該資料受託運用者在執行資料運用活動時，仍須遵守 GDPR 規範之受託運用者義務。

When it comes to a data processor established in the Union carrying out processing on behalf of a data controller with no establishment in the Union for the purpose of the processing activity and which does not fall under the territorial scope of the GDPR as per Article 3(2), the processor will be subject to the following relevant GDPR provisions directly applicable to data processors:
當位於歐盟境內之資料受託運用者，為運用活動之目的，代表於歐盟境內並未設置據點且依據第 3 條第 2 項不屬於 GDPR 地域範圍之控管者執行資料運用時，資料受託運用者將直接受以下 GDPR 相關條文約束：

- The obligations imposed on processors under Article 28 (2), (3), (4), (5) and (6), on the duty to enter into a data processing agreement, with the exception of those relating to the assistance to the data controller in complying with its (the controller's) own obligations under the GDPR.
- 依據第 28 條第 2、3、4、5 和第 6 項負有簽訂資料運用契約之義務，但為協助資料控管者遵守其 GDPR 下之義務時，不在此限。

- The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, as per Article 29 and Article 32(4).
- 受託運用者或在控管者或受託運用者授權下行事之任何人，其雖有權限存取個人資料，但除經資料控管者指示，或依據第 29 條以及第 32 條第 4 項受到歐盟法律或成員國法律之要求，不得運用個人資料。

- Where applicable, the processor shall maintain a record of all categories of processing carried out on behalf of a controller, as per Article 30(2).
- 若適用，依據第 30 條第 2 項，受託運用者應保留代表控管者所為之所有類別運用活動之記錄。

- Where applicable, the processor shall, upon request, cooperate with the supervisory authority in the performance of its tasks, as per Article 31.
- 若適用，依據第 31 條，受託運用者應依要求，與監管機關合作執行其任務。

- The processor shall implement technical and organisational measures to ensure a level of security appropriate to the risk, as per Article 32.
- 依據第 32 條，受託運用者應採取技術性及組織性之措施，以確保符合風險的安全程度。

- The processor shall notify the controller without undue delay after becoming aware of a personal data breach, as per Article 33.
- 依據第 33 條，受託運用者應在知悉個人資料侵害事件後通知控管者，不得無故遲延。

- Where applicable, the processor shall designate a data protection officer as per Articles 37 and 38.
- 若適用，依據第 37 條及第 38 條，受託運用者應指定個資保護長。

- The provisions on transfers of personal data to third countries or international organisations, as per Chapter V.
- 依據第 5 章傳輸個人資料至第三國或國際組織之規定。

In addition, since such processing would be carried out in the context of the activities of an establishment of a processor in the Union, the EDPB recalls that the processor will have to ensure its processing remains lawful with regards to other obligations under EU or national law. Article 28(3) also specifies that "*the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.*"
此外，由於資料運用活動係由受託運用者設立於歐盟境內之據點於其活動範圍內所執行，EDPB 認為，受託運用者必須確保該運用符合歐盟或國家法律下之其他義務。第 28 條第 3 項規定「*若受託運用者認為某指令違反本規則或其他歐盟或成員國資料保護規定時，應立即通知控管者*」。

In line with the positions taken previously by the Article 29 Working Party, the EDPB takes the view that the Union territory cannot be used as a "data haven", for instance when a processing activity entails inadmissible ethical issues[19], and that certain legal obligations beyond the application of EU data protection law, in particular European and national rules with regard to public order, will in any case have to be respected by any data processor established in the Union, regardless of the location of the data controller. This consideration also takes into account the fact that by implementing EU law, provisions resulting from the GDPR and related national laws, are subject to the Charter of Fundamental Rights of the Union[20]. However, this does not impose additional obligations on controllers outside the Union in respect of processing not falling under the territorial scope of the GDPR.
與第 29 條工作小組採取相同之立場，EDPB 認為，歐盟的領域不得作為「資料避難所」，例如運用活動涉及不可接受的道德問題 [19]，以及某些法律義務超出歐盟個人資料保護法所涵蓋之範圍，尤其是涉及歐盟和成員國有關公共秩序法律時，無論資料控管者所在地為何，設立於歐盟境內之資料受託運用者皆需尊重上揭規則。此概念亦考量到在執行歐盟律法時，無論是 GDPR 或成員國之國內法皆受到歐盟基本權利憲章 [20] 之約束。然而，就非屬於 GDPR 地域範圍之運用，此規範對非設立於歐盟境內之控管者不附加額外義務。

[19] G29WP169 - Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16th February 2010
G29WP169 – 意見1/2010 定義「資料控管者」與「資料受託運用者」，於2010年2月16日通過。
[20] Charter of Fundamental Right of the European Union, 2012/C 326/02.
歐盟基本權利憲章，2012/C 326/02。

2. APPLICATION OF THE TARGETING CRITERION – ART 3(2)

第 3 條第 2 項特定目標準則之適用

The absence of an establishment in the Union does not necessarily mean that processing activities by a data controller or processor established in a third country will be excluded from the scope of the GDPR, since Article 3(2) sets out the circumstances in which the GDPR applies to a controller or processor not established in the Union, depending on their processing activities.
在歐盟境內未設立據點並不一定表示設立於第三國之資料控管者或受託運用者之運用活動將被排除於 GDPR 之規範，因為第 3 條第 2 項設置了一些情況，依個人資料運用活動之情形，GDPR 可適用於非設立於歐盟境內之控管者或受託運用者。

In this context, the EDPB confirms that in the absence of an establishment in the Union, a controller or processor cannot benefit from the one-stop shop mechanism provided for in Article 56 of the GDPR. Indeed, the GDPR's cooperation and consistency mechanism only applies to controllers and processors with an establishment, or establishments, within the European Union[21].
承上，EDPB 確認若於歐盟境內未設有據點，資料控管者或受託運用者無法受益於 GDPR 第 56 條所規定之一站式（one-stop shop）機制。實際上，GDPR 的合作和一致性機制僅適用於在歐盟境內設有單一或多個據點之資料控管者及受託運用者[21]。

While the present guidelines aim to clarify the territorial scope of the GDPR, the EDPB also wish to stress that controllers and processors will also need to take into account other applicable texts, such as for instance EU or Member States' sectorial legislation and national laws. Several provisions of the GDPR indeed allow Member States to introduce additional conditions and to define a specific data protection framework at national level in certain areas or in relation to specific processing situations. Controllers and processors must therefore ensure that they are aware of, and comply with, these additional conditions and frameworks which may vary from one Member State to the other. Such variations in the data protection provisions applicable in each Member State are particularly notable in relation to the provisions of Article 8 (providing that the age at which children may give valid consent in relation to the processing of their data by

[21] WP244, 13th December 2016, Guidelines for identifying a controller or processor's lead supervisory authority.
WP244，確認控管者或受託運用者的主要監管機關之指引，於2016年12月13日通過。

information society services may vary between 13 and 16), of Article 9 (in relation to the processing of special categories of data), Article 23 (restrictions) or concerning the provisions contained in Chapter IX of the GDPR (freedom of expression and information; public access to official documents; national identification number; employment context; processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; secrecy; churches and religious associations).

雖然現有指引旨在澄清 GDPR 的地域範圍，但 EDPB 亦希望強調控管者和受託運用者必須考量其它可適用之法規，例如歐盟或其成員國之部門立法和國家法律。GDPR 若干條款均實際上允許成員國制定額外要件，並於某些特定領域或關於特定之資料運用情形，允許成員國定義國家層級之個人資料保護體系。因此，控管者及受託運用者必須確保對該額外要件和體制之瞭解與遵守，而這些額外要件和體制或因各成員國而異。各成員國對於個人資料保護規則之相異性，於下列幾項條款尤其值得注意。第 8 條（規定關於兒童對資訊社會服務運用其個人資料可給予有效同意之年齡，此年齡可介於 13 至 16 歲之間），第 9 條（關於特殊類型之個人資料運用），第 23 條（限制），或關於 GDPR 第 9 章之相關規定（言論及資訊自由；官方文件之公眾取得；國民身分證統一編號； 僱傭關係；為實現公共利益、科學或歷史研究目的或統計目的所為之資料運用；保密；教會及宗教組織）。

Article 3(2) of the GDPR provides that "*this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*"

GDPR 第 3 條第 2 項規定「*本規則適用於非設立於歐盟境內之資料控管者或受託運用者對位於歐盟境內之當事人所為涉及如下事項之個人資料運用：(a) 對歐盟境內之當事人提供商品或服務，不問是否需要當事人付款;或 (b) 監控當事人於歐盟境內之行為*」。

The application of the "targeting criterion" towards data subjects who are in the Union, as per Article 3(2), can be triggered by processing activities carried out by a controller or processor not established in the Union which relate to two distinct and alternative types of activities provided that these processing activities relate to data subjects that are in the Union. In addition to being applicable only to processing by a controller or processor not established in the Union, the targeting criteria largely focuses on what the "processing activities" are "related to", which is to be considered on a case-by-case

basis.
依據第 3 條第 2 項，當運用活動與位於歐盟境內之當事人相關時，對位於歐盟境內之當事人的「特定目標準則」（targeting criterion）適用，係由非設立於歐盟境內之控管者或受託運用者所為相關兩種不同且二擇一之資料運用活動引發適用。除僅適用於資料控管者或受託運用者未設立於歐盟境內之運用，特定目標準則主要關注於與「資料運用活動」「相關」之內容，此須根據具體個案情況加以考量。

The EDPB stresses that a controller or processor may be subject to the GDPR in relation to some of its processing activities but not subject to the GDPR in relation to other processing activities. The determining element to the territorial application of the GDPR as per Article 3(2) lies in the consideration of the processing activities in question.
EDPB強調，控管者或受託運用者某些運用活動可能受拘束於GDPR，而其他運用活動則不受GDPR之拘束。依據第3條第2項，GDPR在地域範圍適用之決定性因素在於就系爭運用活動之考量。

In assessing the conditions for the application of the targeting criterion, the EDPB therefore recommends a twofold approach, in order to determine first that the processing relates to personal data of data subjects who are in the Union, and second whether processing relates to the offering of goods or services or to the monitoring of data subjects' behaviour in the Union.
因此，在分析目標性準則適用條件時，EDPB 建議採用一種二重判斷法。第一需先確認與資料運用相關之當事人係位於歐盟境內，第二需認定此運用是否與提供商品或服務或監控當事人於歐盟內之行為相關。

a) Data subjects in the Union
a) 位於歐盟境內之當事人

The wording of Article 3(2) refers to "*personal data of data subjects who are in the Union*". The application of the targeting criterion is therefore not limited by the citizenship, residence or other type of legal status of the data subject whose personal data are being processed. Recital 14 confirms this interpretation and states that "*[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data*".
第 3 條第 2 項適用於「*歐盟境內當事人之個人資料*」。因此，特定目標準則的適用不受限於當事人之公民身分、居住地或其他類型的法律地位的限制。前言第 14 點確認此種解釋，並指出「*本規則所保護者應適用於自然人，係不論當事人之國籍或居住所，凡涉及其個人資料之運用均屬之*」。

This provision of the GDPR reflects EU primary law which also lays down a broad scope for the protection of personal data, not limited to EU citizens, with Article 8 of the Charter of Fundamental Rights providing that the right to the protection of personal data is not limited but is for "everyone"[22].
GDPR 此規定反映了歐盟主要法律廣泛保護個人資料，不限於歐盟公民，歐洲聯盟基本權利憲章第 8 條規定個人資料受保護之權利沒有限制，且適用於「每個人」[22]。

While the location of the data subject in the territory of the Union is a determining factor for the application of the targeting criterion as per Article 3(2), the EDPB considers that the nationality or legal status of a data subject who is in the Union cannot limit or restrict the territorial scope of the Regulation.
依據第 3 條第 2 項，雖然當事人位於歐盟之位置是適用特定目標準則的決定要素，但 EDPB 認為，位於歐盟境內當事人之國籍或法律地位並不限縮本規則之地域範圍。

The requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken.
當事人位於歐盟境內要件之評估，應根據相關觸發活動發生的時點，也就是提供商品或服務或監控當事人行為的時點，不論此供給或監控的持續時間有多長。

The EDPB considers however that, in relation to processing activities related to the offer of services, the provision is aimed at activities that intentionally, rather than inadvertently or incidentally, target individuals in the EU. Consequently, if the processing relates to a service that is only offered to individuals outside the EU but the service is not withdrawn when such individuals enter the EU, the related processing will not be subject to the GDPR. In this case the processing is not related to the intentional targeting of individuals in the EU but relates to the targeting of individuals outside the EU which will continue whether they remain outside the EU or whether they visit the Union.
然而，EDPB 認為，就與服務提供相關之運用活動而言，該規定之目的旨在規範有意以位於歐盟當事人之活動為特定目標，而非無意或偶然之情形。因此，若運用僅涉及向位於歐盟外之個人提供服務，但當該個人進入歐盟時並未撤回該服務，則相關運用將不受 GDPR 拘束。在此情況下，運用與以位於歐盟境內之個人為特

[22] Charter of Fundamental Right of the European Union, Article 8(1), « Everyone has the right to the protection of personal data concerning him or her".
歐盟基本權利憲章第8條「每個人皆有權利保護與自身相關之個人資料」。

定目標之情形無關，而是與以位於歐盟外之個人為特定目標相關，無論該個人是否留在歐盟境外抑或參訪歐盟，此種運用都將持續進行。

Example 8: An Australian company offers a mobile news and video content service, based on user's preferences and interests. Users can receive daily or weekly updates. The service is offered exclusively to users located in Australia, who must provide an Australian phone number when subscribing.
示例 8：一家澳大利亞公司依據用戶偏好和興趣提供行動新聞和影音內容服務。用戶可接收每日或每週更新。該服務是專為位於澳大利亞之用戶所提供，用戶在訂閱時必須提供澳大利亞之電話號碼。

An Australian subscriber of the service travels to Germany on holiday and continues using the service.
訂閱該服務的澳大利亞用戶在假日時前往德國旅遊，並繼續使用該服務。

Although the Australian subscriber will be using the service while in the EU, the service is not 'targeting' individuals in the Union, but targets only individuals in Australia, and so the processing of personal data by the Australian company does not fall within the scope of the GDPR.
儘管澳大利亞用戶將在歐盟境內使用該服務，但該服務並非以位於歐盟之個人「為特定目標」，而是僅以位於澳大利亞之個人為目標，因此，澳大利亞公司對個人資料之運用不屬於 GDPR 之適用範圍。

Example 9: A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The application processes personal data concerning the location of customers using the app (the data subjects) once they start using the application in the city they visit, in order to offer targeted advertisement for places to visits, restaurant, bars and hotels. The application is available for tourists while they visit New York, San Francisco, Toronto, London, Paris and Rome.
示例 9：一家設立於美國且在歐盟沒有任何商業活動或據點的新創公司，為遊客提供城市地圖的應用程式。為了向遊客提供所在城市有關旅遊地點、餐館、酒吧和旅館的針對性廣告，當用戶（當事人）開始使用地圖服務時，應用程式便會對用戶之所在位置進行個人資料運用。該應用程式提供遊客於參訪紐約、舊金山、多倫多、倫敦、巴黎和羅馬等城市時之地圖服務。

The US start-up, via its city mapping application, is specifically targeting individuals in the Union (namely in Paris and Rome) through offering its services to them when they

are in the Union. The processing of the EU-located data subjects' personal data in connection with the offering of the service falls within the scope of the GDPR as per Article 3(2)a. Furthermore, by processing data subject's location data in order to offer targeted advertisement on the basis of their location, the processing activities also relate to the monitoring of behaviour of individuals in the Union. The US start-up processing therefore also falls within the scope of the GDPR as per Article 3(2)b.
該美國新創公司透過其城市地圖應用程式，特別以歐盟境內（即巴黎和羅馬）之個人為目標，當用戶位於歐盟時為其提供服務。依據第 3 條第 2 項第 a 款，為提供其服務而運用位於歐盟境內當事人之個人資料，屬於 GDPR 之適用範圍。此外，當透過運用個資當事人之定位資料以便依據其所在地提供針對性廣告時，該運用活動亦涉及對位於歐盟境內個人行為之監控。因此，依據第 3 條第 2 項第 b 款，美國新創公司之運用活動亦屬於 GDPR 之適用範圍。

The EDPB also wishes to underline that the fact of processing personal data of an individual in the Union alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the Union. The element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour (as further clarified below), must always be present in addition.
EDPB 強調，對非設立於歐盟境內的控管者或受託運用者，僅以其運用位於歐盟境內個人資料的事實，尚不足以觸發 GDPR 的適用。無論係透過提供商品或服務，亦或透過監控當事人的行動（如下文進一步闡明），皆以位於歐盟之個人為「特定目標」做為額外要件。

Example 10: A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market, evident by the app terms of use and the indication of US Dollar as the sole currency available for payment. The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR.
示例 10：一個美國公民在假期間前往歐洲旅行。 在歐洲期間，他下載並使用由美國公司提供的新聞應用程式。鑑於該應用程式之使用條款及以美元為唯一可支付貨幣，該應用程式僅針對美國市場。美國公司通過應用程式蒐集美國旅客的個人資料不受 GDPR 拘束。

Moreover, it should be noted that the processing of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR, as long as the processing is not related to a specific offer directed at individuals in the EU or to a monitoring of their behaviour in the Union.
再者，針對位於第三國的歐盟公民或居民所為之資料運用行為，只要該資料運用

與提供位於歐盟內當事人商品或服務或監控其行動無關，則不會觸發 GDPR 的適用。

Example 11: A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship. The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.
示例 11：一家位於臺灣的銀行，其客戶雖居住於臺灣，但持有德國國籍。該銀行的活動範圍僅限於臺灣而非針對歐盟市場。位於臺灣的銀行運用德國客戶的個人資料不受 GDPR 拘束。

Example 12: The Canadian immigration authority processes personal data of EU citizens when entering the Canadian territory for the purpose of examining their visa application. This processing is not subject to the GDPR.
示例 12：加拿大移民署在歐盟公民進入加拿大領土時，運用歐盟公民的個人資料，以審查其簽證申請。此運用不受 GDPR 拘束。

b) Offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union
b) 對位於歐盟境內的當事人提供商品或服務，不問是否需要當事人付款

The first activity triggering the application of Article 3(2) is the "offering of goods or services", a concept which has been further addressed by EU law and case law, which should be taken into account when applying the targeting criterion. The offering of services also includes the offering of information society services, defined in point (b) of Article 1(1) of Directive (EU) 2015/1535[23] as "*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".
觸發第 3 條第 2 項適用的第一種行為係「提供商品或服務」，歐盟法律和判例法進一步說明此一概念，又此行為須將特定目標準則納入考量。提供的服務也包括提供資訊社會服務（Information society service），歐盟指令 2015/1535 第 1 條第 1

[23] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.
歐洲議會和歐盟理事會於2015年9月9日所發布之第2015/1535號指令（EU），規定了在技術法規和資訊社會服務規則領域提供資訊之程序。

項 b 款定義該服務為「*以報酬為目的，在一定距離外，依據服務接受者的個人要求以電子方式提供資訊社會服務*」。

Article 3(2)(a) specifies that the targeting criterion concerning the offering of goods or services applies irrespective of whether a payment by the data subject is required. Whether the activity of a controller or processor not established in the Union is to be considered as an offer of a good or a service is not therefore dependent whether payment is made in exchange for the goods or services provided[24].
第 3 條第 2 項第 a 款特別規定，特定目標準則適用於提供商品或服務，不問是否需要當事人付款。因此，非設立於歐盟境內之控管者或受託運用者的活動，是否得被視為提供商品或服務，與是否需付費以交換該商品或服務之提供無關[24]。

Example 13: A US company, without any establishment in the EU, processes personal data of its employees that were on a temporary business trip to France, Belgium and the Netherlands for human resources purposes, in particular to proceed with the reimbursement of their accommodation expenses and the payment of their daily allowance, which vary depending on the country they are in.
示例 13：一家在歐盟沒有任何據點的美國公司，基於人力資源目的，當其員工暫時去法國、比利時和荷蘭出差時，運用此些員工之個人資料，尤其係為給付住宿費用和每日津貼，具體費用視員工所在國家而定。

In this situation, while the processing activity is specifically connected to persons on the territory of the Union (i.e. employees who are temporarily in France, Belgium and the Netherlands) it does not relate to an offer of a service to those individuals, but rather is part of the processing necessary for the employer to fulfil its contractual obligation and human resources duties related to the individual's employment. The processing activity does not relate to an offer of service and is therefore not subject to the provision of the GDPR as per Article 3(2)a.
於此情況下，雖然運用活動特定與位於歐盟境內之人員（即暫時位於法國、比利時和荷蘭之員工）相關，然該運用與向此些人員提供服務無關，而是雇主為履行與個人僱傭相關之契約義務及人力資源職責所必需之運用。該運用活動與服務提供無關，依據第 3 條第 2 項第 a 款之規定，因此不受 GDPR 之拘束。

Another key element to be assessed in determining whether the Article 3(2)(a) targeting criterion can be met is whether the offer of goods or services is directed at a person in the Union, or in other words, whether the conduct on the part of the controller, which

[24] See, in particular, CJEU, C-352/85, Bond van Adverteerders and Others vs. The Netherlands State, 26 April 1988, par. 16), and CJEU, C-109/92, Wirth [1993] Racc. I-6447, par. 15.
特別參閱歐盟法院C-352/85，Bond van Adverteerders和Others vs. The Netherlands State，1988年4月26日，段落16和歐盟法院C-109/92，Wirth [1993] Racc. I-6447，段落15。

determines the means and purposes of processing, demonstrates its intention to offer goods or a services to a data subject located in the Union. Recital 23 of the GDPR indeed clarifies that "*in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.*"
在確認第 3 條第 2 項 a 款特定目標準則時，另一項評估關鍵要素為，商品或服務之提供是否係針對位於歐盟境內之當事人。換句話說，決定運用方式及目的之控管者之行為是否表明其有意圖對位於歐盟的當事人提供商品或服務。GDPR 前言第 23 點闡明「*為決定控管者或受託運用者是否為歐盟境內之當事人提供商品或服務，應確認是否明顯可知該控管者或受託運用者預見其係提供服務予位於一個或多個歐盟會員國境內之當事人*」。

The recital further specifies that "*whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.*"
前言第 23 點進一步說明「*若僅係可接近使用控管者、受託運用者或中介者於歐盟內之網頁、電子郵件或其他聯繫方式，或使用之語言係控管者設立地之第三國所通常使用之語言，均不足以確認其具有提供商品或服務之意圖；但其他要素諸如：所使用之語言或貨幣通常係使用於一個或多個會員國境內且有以該語言訂購商品或服務之可能性，或所提及之消費者或使用者位於歐盟境內，則可能使其明顯可知控管者擬向位於歐盟境內之當事人提供商品或服務。*」

The elements listed in Recital 23 echo and are in line with the CJEU case law based on Council Regulation 44/2001[25] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, and in particular its Article 15(1)(c). In *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (Joined cases C-585/08 and C-144/09), the Court was asked to clarify what it means to "direct activity" within the meaning of Article 15(1)(c) of Regulation 44/2001 (*Brussels I*). The CJEU held that, in order to determine whether a trader can be considered to be

[25] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
2000年12月22日歐盟理事會條例（EC）第44/2001號，關於民事和商業事務中管轄權以及判決之承認和執行。

"directing" its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Brussels I, the trader must have manifested its intention to establish commercial relations with such consumers. In this context, the CJEU considered evidence able to demonstrate that the trader was envisaging doing business with consumers domiciled in a Member State.

前言第23點所列舉之要素與歐盟法院基於第44/2001[25]號規則就管轄權以及承認與執行民商事判決的判例法一致，特別是第 15 條第 1 項 c 款之規定。在 *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (合併案件 C-585/08 and C-144/09)中，法院被要求澄清第 44/2001 號規則（*布魯塞爾 I*）第 15 條第 1 項 c 款中「活動指向」（direct activity）之定義。歐盟法院認為，在布魯塞爾 I 第 15 條第 1 項 c 款的涵義內，為決定貿易商是否得被認定將其活動「指向」到消費者住所地之成員國，貿易商必須表明與消費者建立商業關係之意圖。在此情形下，歐盟法院認為證據足資證明貿易商預計和居住於成員國之消費者做生意。

While the notion of "directing an activity" differs from the "offering of goods or services", the EDPB deems this case law in in *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller (Joined cases C-585/08 and C-144/09)*[26]might be of assistance when considering whether goods or services are offered to a data subject in the Union. When taking into account the specific facts of the case, the following factors could therefore *inter alia* be taken into consideration, possibly in combination with one another:

雖然「活動指向」的概念與「提供商品或服務」不同，但 EDPB 認為，*Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller (合併案件 C-585/08 and C-144/09)*[26] 一案對釐清是否向歐盟境內的當事人提供商品或服務的定義可能有所助益。因此，*除其他事項*，在考量案件之具體事實時，可交叉比對以下要素：

- The EU or at least one Member State is designated by name with reference to the good or service offered;

- 所提供之商品或服務以名稱指定歐盟或至少一個成員國為其標的；

- The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns

[26] It is all the more relevant that, under Article 6 of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), in absence of choice of law, this criterion of "directing activity" to the country of the consumer's habitual residence is taken into account to designate the law of the consumer's habitual residence as the law applicable to the contract.

依據歐洲議會和歐盟理事會2008年6月17日第593/2008（EC）號規則第6條關於契約義務準則（羅馬I），若無法律選擇之適用，「活動指向準則」將消費者居住國納入考量，以指定消費者住所地之法律適用於契約。

directed at an EU country audience;
- 資料控管者或受託運用者向搜索引擎運營商付費取得網路參考服務，以利位於歐盟境內之消費者得造訪其網站；或控管者或受託運用者針對位於歐盟的觀眾啟動行銷和廣告活動；

- The international nature of the activity at issue, such as certain tourist activities;
- 活動的國際性質，例如特定之旅遊活動；

- The mention of dedicated addresses or phone numbers to be reached from an EU country;
- 提供位於歐盟某一國家境內可供聯繫的專用地址或電話號碼；

- The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example ".de", or the use of neutral top-level domain names such as ".eu";
- 資料控管者或受託運用者未使用所在地第三國之頂級網域名稱，卻使用如「.de」，或使用中性頂級網域名稱，如「.eu」；

- The description of travel instructions from one or more other EU Member States to the place where the service is provided;
- 提供一個或多個歐盟成員國到其服務提供地的旅行指示說明；

- The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;
- 提及居住於不同歐盟成員國境內客戶組成的國際客戶，尤其是提供由此類客戶所撰寫之帳戶資料；

- The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states;
- 使用貿易商所在國家以外的語言或貨幣，尤其是使用一個或多個歐盟成員國的語言或貨幣；

- The data controller offers the delivery of goods in EU Member States.
- 資料控管者提供貨物運送至歐盟成員國。

As already mentioned, several of the elements listed above, if taken alone may not amount to a clear indication of the intention of a data controller to offer goods or services to data subjects in the Union, however, they should each be taken into account in any in *concreto* analysis in order to determine whether the combination of factors relating to the data controller's commercial activities can together be considered as an

offer of goods or services directed at data subjects in the Union.
若單獨考慮前述幾項要件，可能無法清楚指出資料控管者提供位於歐盟境內當事人商品或服務之意圖。然而，在*具體分析*中，為決定資料控管者的整體商業活動是否可被視為係直接針對位於歐盟境內之當事人所提供之商品或服務，每一項要件都應列入考量範圍內。

It is however important to recall that Recital 23 confirms that the mere accessibility of the controller's, processor's or an intermediary's website in the Union, the mention on the website of its e-mail or geographical address, or of its telephone number without an international code, does not, of itself, provide sufficient evidence to demonstrate the controller or processor's intention to offer goods or a services to a data subject located in the Union. In this context, the EDPB recalls that when goods or services are inadvertently or incidentally provided to a person on the territory of the Union, the related processing of personal data would not fall within the territorial scope of the GDPR.
需再次強調，前言第 23 點確認，單純於歐盟內造訪資料控管者、受託運用者或中間商的網站，在網站上提及電子郵件或區域地址，或提及沒有國際代碼的電話號碼，皆無法提供足夠的證據來證明控管者或受託運用者有意圖對位於歐盟境內的當事人提供商品或服務。於此情況下，EDPB 重申，若無意或偶然地向位於歐盟領域內之個人提供了商品或服務，則與該個人資料相關之運用將不屬於 GDPR 之地域範圍。

Example 14: A website, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros. The website indicates that photo albums can only be delivered by post mail in the UK, France, Benelux countries and Germany.
示例 14：設立與管理皆位於土耳其的網站，為個性化家庭相冊的創建、編輯、印刷和運送提供服務。該網站提供英語、法語、荷蘭語和德語版本，且可使用歐元付款。該網站表明，相冊只能透過郵寄方式在英國、法國、比荷盧聯盟國家和德國運送。

In this case, it is clear that the creation, editing and printing of personalised family photo albums constitute a service within the meaning of EU law. The fact that the website is available in four languages of the EU and that photo albums can be delivered by post in six EU Member States demonstrates that there is an intention on the part of the Turkish website to offer its services to individuals in the Union.
在此案例中，個性化家庭相冊的創建、編輯和印刷明顯屬於歐盟法律定義上之服

務。網站提供四種於歐盟內使用的語言，相冊可郵寄於六個歐盟成員國，皆表明該土耳其網站有意圖向位於歐盟境內之個人提供服務。

As a consequence, it is clear that the processing carried out by the Turkish website, as a data controller, relates to the offering of a service to data subjects in the Union and is therefore subject to the obligations and provisions of the GDPR, as per its Article 3(2)(a).
因此，顯然該土耳其網站，作為資料控管者所執行的資料運用，涉及向歐盟境內的當事人提供服務，因此依據第 3 條第 2 項 a 款，需遵守 GDPR 的義務和規範。

In accordance with Article 27, the data controller will have to designate a representative in the Union.
依據第 27 條，資料控管者必須於歐盟境內指定代表人。

Example 15: A private company based in Monaco processes personal data of its employees for the purposes of salary payment. A large number of the company's employees are French and Italian residents.
示例 15：某位於摩納哥的私人公司為支付工資而運用其員工的個人資料。 該公司的大量員工是位於法國和義大利的居民。

In this case, while the processing carried out by the company relates to data subjects in France and Italy, it does not takes place in the context of an offer of goods or services. Indeed human resources management, including salary payment by a third-country company cannot be considered as an offer of service within the meaning of Art 3(2)a. The processing at stake does not relate to the offer of goods or services to data subjects in the Union (nor to the monitoring of behaviour) and, as a consequence, is not subject to the provisions of the GDPR, as per Article 3.
於此案例中，雖然公司執行的資料運用涉及位於法國和義大利的當事人，但該運用並不是以提供商品或服務為目的。實際上，人力資源管理，包括第三國公司工資之支付，不屬於第 3 條第 2 項 a 款所意指之服務提供。係爭運用行為與提供歐盟境內的當事人商品或服務（或行為監控）無關，因此，根據第 3 條，該運用不受 GDPR 規範之拘束。

This assessment is without prejudice to the applicable law of the third country concerned.
此評估不妨礙第三國的法律適用。

Example 16: A Swiss University in Zurich is launching its Master degree selection process, by making available an online platform where candidates can upload their CV and cover letter, together with their contact details. The selection process is open to any student with a sufficient level of German and English and holding a Bachelor degree. The University does not specifically advertise to students in EU Universities, and only takes payment in Swiss currency.

示例 16：蘇黎世的瑞士大學正推出碩士學位甄選程序，透過網站，候選人可上傳簡歷和自薦信，以及聯繫方式。甄選程序開放於任何具有合格德語和英語能力且持有學士學位的學生。該大學沒有專門向歐盟大學的學生宣傳，且只接受瑞士貨幣的支付。

As there is no distinction or specification for students from the Union in the application and selection process for this Master degree, it cannot be established that the Swiss University has the intention to target students from a particular EU member states. The sufficient level of German and English is a general requirement that applies to any applicant whether a Swiss resident, a person in the Union or a student from a third country. Without other factors to indicate the specific targeting of students in EU member states, it therefore cannot be established that the processing in question relates to the offer of an education service to data subject in the Union, and such processing will therefore not be subject to the GDPR provisions.

碩士學位的申請和甄選程序並沒有針對位於歐盟境內的學生，因此無法認定瑞士大學有意圖將特定歐盟成員國的學生列為目標。合格的德語和英語能力要件適用於任何申請人，無論是瑞士居民、歐盟申請人或是來自第三國的學生。若無其他因素表明該甄選程序係針對歐盟成員國的學生，資料的運用不得被視為涉及向位於歐盟境內之當事人提供教育服務，因此該運用不屬於 GDPR 的適用範圍。

The Swiss University also offers summer courses in international relations and specifically advertise this offer in German and Austrian universities in order to maximise the courses' attendance. In this case, there is a clear intention from the Swiss University to offer such service to data subjects who are in the Union, and the GDPR will apply to the related processing activities.

瑞士大學另外提供國際關係的暑期課程，為了大幅提高參與人數，在德國和奧地利的大學中特別宣傳此課程。在此情況下，瑞士大學明確有意圖向位於歐盟境內當事人提供此類服務，因此 GDPR 將適用於相關的運用活動。

c) Monitoring of data subjects' behaviour

c）監控當事人之行為

The second type of activity triggering the application of Article 3(2) is the monitoring of data subject behaviour as far as their behaviour takes place within the Union.
觸發第 3 條第 2 項適用之第二類活動是監控當事人位於歐盟境內所為之行為。

Recital 24 clarifies that "*[t]he processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.*"
前言第 24 點闡明「*凡為歐盟境內之當事人，雖由非設立於歐盟境內之控管者或受託運用者進行個人資料運用，惟其涉及對該當事人之行為所為監控且該受監控之行為係發生於歐盟境內者，本規則亦應予適用。*」

For Article 3(2)(b) to trigger the application of the GDPR, the behaviour monitored must first relate to a data subject in the Union and, as a cumulative criterion, the monitored behaviour must take place within the territory of the Union.
為第 3 條第 2 項 b 款觸發 GDPR 之適用，受監控之行為首先必須與位於歐盟境內之當事人相關，且該行為必須發生於歐盟的領土內。

The nature of the processing activity which can be considered as behavioural monitoring is further specified in Recital 24 which states that "*in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.*" While Recital 24 exclusively relates to the monitoring of a behaviour through the tracking of a person on the internet, the EDPB considers that tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioural monitoring, for example through wearable and other smart devices.
前言第 24 點進一步闡明可被視為行為監控之資料運用活動之性質。該項前言指出「*為決定該資料運用是否可受認定為監控該當事人之行為，應確認該當事人是否於網路上被追蹤，包含以個人資料運用技術對自然人進行剖析的潛在後續利用，尤其是為了作成與其有關的決策，或為分析或預測其個人偏好、行為及態度*」。雖然前言第 24 點針對涉及透過網路追蹤當事人之行為監控，但 EDPB 認為在確認運用活動是否可被視為行為監控時，亦應考量藉由其他類型的網路或技術所為之追蹤而涉及的資料運用。例如透過可穿戴和其他智能設備進行之行為監控。

As opposed to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24

expressly introduce a necessary degree of “intention to target” on the part of the data controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities. However, the use of the word “monitoring” implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual’s behaviour within the EU. The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as “monitoring”. It will be necessary to consider the controller’s purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes into account the wording of Recital 24, which indicates that to determine whether processing involves monitoring of a data subject behaviour, the tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration.

與第 3 條第 2 項 a 款的規定不同，第 3 條第 2 項 b 款和前言第 24 點在確認監控活動是否屬於資料運用而觸發 GDPR 的適用時，皆未明確規範資料控管者或受託運用者須具備必要程度的「特定目標意圖」。然而，使用「監控」一詞，意味著控管者心中有一特定目的，以蒐集和後續使用位於歐盟境內當事人行為的相關數據。EDPB 不認為任何線上蒐集或分析位於歐盟境內個人的資料皆自動視為「監控」。控管者進行資料運用之目的必須列入考量，特別是任何後續行為分析或相關資料之剖析技術。參照前言第 24 點，EDPB 認為，為了確認資料運用是否涉及監控當事人的行為，追蹤網路上的自然人，包括後續使用剖析技術之可能性，係關鍵考量要素。

The application of Article 3(2)(b) where a data controller or processor monitors the behaviour of data subjects who are in the Union could therefore encompass a broad range of monitoring activities, including in particular:

因此，第 3 條第 2 項 b 款之適用，對於資料控管者或受託運用者監控位於歐盟境內當事人之行為，可能涵蓋廣泛的監控活動，特別包括：

- Behavioural advertisement
- 行為廣告

- Geo-localisation activities, in particular for marketing purposes
- 地理定位活動，特別是針對於行銷目的

- Online tracking through the use of cookies or other tracking techniques such as fingerprinting
- 透過使用 cookie 或其他追蹤技術（如數位指紋）所進行之線上追蹤

- Personalised diet and health analytics services online
- 線上個別化飲食和健康分析服務

- CCTV
- 閉路電視

- Market surveys and other behavioural studies based on individual profiles
- 基於個人檔案所進行之市場調查和其他行為研究

- Monitoring or regular reporting on an individual's health status
- 對個人的健康狀況進行監控或定期報告

Example 17: A retail consultancy company established in the US provides advice on retail layout to a shopping centre in France, based on an analysis of customers' movements throughout the centre collected through Wi-Fi tracking.
示例 17：設立於美國的一間零售諮詢公司透過 Wi-Fi，追蹤蒐集購物中心客戶行動分析，並向位於法國的購物中心提供零售佈置設計建議。

The analysis of a customers' movements within the centre through Wi-Fi tracking will amount to the monitoring of individuals' behaviour. In this case, the data subjects' behaviour takes place in the Union since the shopping centre is located in France. The consultancy company, as a data controller, is therefore subject to the GDPR in respect of the processing of this data for this purpose as per its Article 3(2)(b).
透過 Wi-Fi 追蹤分析客戶在購物中心內的行動相當於監控個人的行為。於此案例中，由於購物中心位於法國，當事人的行為發生在歐盟境內。因此，依據第 3 條第 2 項 b 款，該作為資料控管者的諮詢公司，就前述目的所為之資料運用行為受 GDPR 拘束。

In accordance with Article 27, the data controller will have to designate a representative in the Union.
依據第 27 條，資料控管者必須於歐盟境內指定代表人。

Example 18: An app developer established in Canada with no establishment in the Union monitors the behaviour of data subject in the Union and is therefore subject to the GDPR, as per Article 3(2)b. The developer uses a processor established in the US for the app optimisation and maintenance purposes.
示例 18：依據第 3 條第 2 項 b 款，位於加拿大的應用程式開發商，雖在歐盟內未設立據點，但監控位於歐盟境內當事人的行為，屬於 GDPR 的適用範圍。 該開發商任用設立於美國的受託運用者進行應用程式的優化和維護。

In relation to this processing, the Canadian controller has the duty to only use appropriate processors and to ensure that its obligations under the GDPR are reflected in the contract or legal act governing the relation with its processor in the US, pursuant to Article 28.
就此資料運用而言，依據第 28 條，加拿大的控管者有責任僅任用適當的受託運用者，並確保其在 GDPR 下所應承擔之義務，於契約或其他法律行為中反映。

d) Processor not established in the Union
d) 非設立於歐盟境內之受託運用者

Processing activities which are “related” to the targeting activity which triggered the application of Article 3(2) fall within the territorial scope of the GDPR. The EDPB considers that there needs to be a connection between the processing activity and the offering of good or service, but both processing by a controller and a processor are relevant and to be taken into account.
當運用活動與觸發第 3 條第 2 項的活動「相關聯」時，亦屬於 GDPR 的地域範圍。EDPB 認為，運用活動與商品或服務的提供之間需有關聯性，但無論係控管者或受託運用者之運用活動，皆需納入考量範圍。

When it comes to a data processor not established in the Union, in order to determine whether its processing may be subject to the GDPR as per Article 3(2), it is necessary to look at whether the processing activities by the processor “are related” to the targeting activities of the controller.
對於非設立於歐盟境內之受託運用者，依據第 3 條第 2 項之規定，為確認其運用是否受拘束於 GDPR，則必須查看該受託運用者之運用活動是否與控管者特定目標性之活動「相關聯」。

The EDPB considers that, where processing activities by a controller relates to the offering of goods or services or to the monitoring of individuals’ behaviour in the Union

('targeting'), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Art 3(2) in respect of that processing.
EDPB 認為，若控管者之運用活動與商品或服務之提供相關或與監控位於歐盟境內個人之行為相關時（「特定目標性」），則任何受指示代表控管者進行運用活動之受託運用者，就該運用而言，依據第 3 條第 2 項，將屬於 GDPR 之適用範圍。

The 'Targeting' character of a processing activity is linked to its purposes and means; a decision to target individuals in the Union can only be made by an entity acting as a controller. Such interpretation does not rule out the possibility that the processor may actively take part in processing activities related to carrying out the targeting criteria (i.e. the processor offers goods or services or carries out monitoring actions on behalf of, and on instruction from, the controller).
運用活動之「特定目標性」特徵與其運用之目的和方式相關；僅有作為控管者之實體，得作出以位於歐盟之個人為目標的決定。此種解釋並不排除受託運用者可能積極參與和執行與目標性準則相關運用活動之可能性。（意即，受託運用者代表控管者並依據其指示提供商品或服務，或執行監控行為）。

The EDPB therefore considers that the focus should be on the connection between the processing activities carried out by the processor and the targeting activity undertaken by a data controller.
因此，EDPB 認為重點應放置於受託運用者所執行之運用活動與資料控管者所執行之特定目標性活動間之關聯性。

Example 19: A Brazilian company sells food ingredients and local recipes online, making this offer of good available to persons in the Union, by advertising these products and offering the delivery in the France, Spain and Portugal. In this context, the company instructs a data processor also established in Brazil to develop special offers to customers in France, Spain and Portugal on the basis of their previous orders and to carry out the related data processing.
示例 19：一家巴西公司在網上出售食材和當地食譜，透過對此些產品之廣告，向位於歐盟境內之個人提供此些商品，並在法國、西班牙和葡萄牙提供送貨服務。在此種情況下，該公司指示同樣設立於巴西之資料受託運用者，依據先前訂購資料，向位於法國、西班牙和葡萄牙之客戶提供特別優惠，並執行相關資料運用。

Processing activities by the processor, under the instruction of the data controller, are related to the offer of good to data subject in the Union. Furthermore, by developing these customized offers, the data processor directly monitors data subjects in the EU.

Processing by the processor are therefore subject to the GDPR, as per Article 3(2).
受託運用者在資料控管者指示下執行之運用活動，與向位於歐盟境內之資料當事人提供商品相關聯。此外，透過建立此些客製化之優惠，資料受託運用者可直接監控位於歐盟境內之資料當事人。因此，依據第 3 條第 2 項，受託運用者所為之運用受 GDPR 所拘束。

Example 20: A US company has developed a health and lifestyle app, allowing users to record with the US company their personal indicators (sleep time, weight, blood pressure, heartbeat, etc …). The app then provide users with daily advice on food and sport recommendations. The processing is carried out by the US data controller. The app is made available to, and is used by, individuals in the Union. For the purpose of data storage, the US company uses a processor established in the US (cloud service provider)
示例 20：一家美國公司開發了一個健康和生活方式應用程式，該程式允許用戶向美國公司記錄其個人指標項目（睡眠時間、體重、血壓、心跳等）。該應用程式而後每日為用戶提供有關食物和運動之建議。該應用程式可提供予且亦被位於歐盟境內之個人使用。為進行資料存儲，該美國公司使用設立於美國境內之受託運用者（雲端服務提供者）

To the extent that the US company is monitoring the behaviour of individuals in the EU, in operating the health and lifestyle app it will be 'targeting' individuals in the EU and its processing of the personal data of individuals in the EU will fall within the scope of the GDPR under Art 3(2).
在美國公司監控位於歐盟境內個人行為之程度上，當操作健康和生活方式應用程式時，該公司將以歐盟境內之個人「為特定目標」，且其運用歐盟境內個人之資料將依據第 3 條第 2 項屬於 GDPR 之適用範圍。

In carrying out the processing on instructions from, and on behalf of, the US company the cloud provider/processor is carrying out a processing activity 'relating to' the targeting of individuals in the EU by its controller. This processing activity by the processor on behalf of its controller falls within the scope of the GDPR under Art 3(2).
在依美國公司之指示並代表美國公司執行運用時，雲端提供商/受託運用者正在執行與其控管者以位於歐盟境內個人為目標所為之運用活動相關聯。受託運用者代表其控管者所為之運用活動依據第 3 條第 2 項屬於 GDPR 之適用範圍。

Example 21: A Turkish company offers cultural package travels in the Middle East with tour guides speaking English, French and Spanish. The package travels are notably advertised and offered through a website available in the three languages, allowing for online booking and payment in Euros and GBP. For marketing and commercial prospection purposes, the company instructs a data processor, a call center, established in Tunisia to contact former customers in Ireland, France, Belgium and Spain in order to get feedback on their previous travels and inform them about new offers and destinations. The controller is 'targeting' by offering its services to individuals in the EU and its processing will fall within the scope of Art 3(2).

示例 21：一家土耳其公司在中東提供文化套餐旅行，其導遊會講英語、法語和西班牙語。該套餐旅行特別以三種語言透過網站進行廣告宣傳和提供服務，且允許以歐元和英鎊線上預訂和付款。為了進行市場行銷和商業勘查，該公司指示設立於突尼西亞之資料受託運用者(一間電話服務中心)，與位於愛爾蘭、法國、比利時及西班牙之先前客戶進行聯繫，以獲取有關其從前旅遊之反饋意見，並告知此些客戶新的優惠和旅遊目的地。控管者透過「特定目標性」，向位於歐盟境內之個人提供服務，其運用將屬於第 3 條第 2 項之適用範圍。

The processing activities of the Tunisian processor, which promotes the controllers' services towards individuals in the EU, is also related to the offer of services by the controller and therefore falls within the scope of Art 3(2). Furthermore, in this specific case, the Tunisian processor actively takes part in processing activities related to carrying out the targeting criteria, by offering services on behalf of, and on instruction from, the Turkish controller.

突尼西亞受託運用者之運用活動，向位於歐盟境內之個人推展了控管者之服務，也與控管者所提供之服務相關，因此屬於第 3 條第 2 項之範圍。此外，在此種特定情況下，突尼西亞受託運用者透過代表土耳其控管者並依據其指示提供服務，積極參與及執行與特定目標準則相關之運用活動。

e) Interaction with other GDPR provisions and other legislations

e）與其他 GDPR 規則及其他法規之相互作用

The EDPB will also further assess the interplay between the application of the territorial scope of the GDPR as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary.

EDPB 亦將進一步評估第 3 條 GDPR 領域範圍之適用與第 5 章國際資料傳輸規範間之相互影響。若有必要，可於此面向發布其他指引。

Controllers or processors not established in the EU will be required to comply with their own third country national laws in relation to the processing of personal data. However, where such processing relates to the targeting of individuals in the Union as per Article 3(2) the controller will, in addition to being subject to its country's national law, be required to comply with the GDPR. This would be the case regardless of whether the processing is carried out in compliance with a legal obligation in the third country or simply as a matter of choice by the controller.

非設立於歐盟境內之控管者或受託運用者將被要求於運用個人資料時遵守其自身之第三國法規。然而，依據第 3 條第 2 項，若此類運用涉及以位於歐盟境內之個人為特定目標，除須遵守其自身國家之國內法規，控管者亦須遵守 GDPR。無論運用係依據第三國之法律義務亦或僅係由控管者之選擇而執行，皆須遵守此規範。

3. PROCESSING IN A PLACE WHERE MEMBER STATE LAW APPLIES BY VIRTUE OF PUBLIC INTERNATIONAL LAW

成員國法律依國際公法可得適用領域內所為之個人資料運用

Article 3(3) provides that "*[t]his Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*". This provision is expanded upon in Recital 25 which states that "*[w]here Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.*"

第 3 條第 3 項規定，「*本規則適用於設立在非歐盟境內，但依國際公法而適用成員國法律之領域的控管者所為之個人資料運用*」。前言第 25 點闡述第 3 條第 3 款之適用，該前言指出「*凡成員國法律依國際公法可得適用之領域，本規則亦應適用於非設立於歐盟境內之控管者，諸如成員國之大使館或領事館*」。

The EDPB therefore considers that the GDPR applies to personal data processing carried out by EU Member States' embassies and consulates located outside the EU as such processing falls within the scope of the GDPR by the virtue of Article 3(3). A Member State's diplomatic or consular post, as a data controller or processor, would then be subject to all relevant provisions of the GDPR, including when it comes to the rights of the data subject, the general obligations related to controller and processor and the transfers of personal data to third countries or international organisations.

因此，EDPB 認為，依據第 3 條第 3 項，若歐盟成員國位於歐盟境外之大使館和領事館所為之個人資料運用屬於 GDPR 之實質範圍，GDPR 即適用於該個人資料運

用。成員國的外交或領事館，作為資料控管者或受託運用者，將受 GDPR 所有相關規定拘束，包括當事人權利、控管者和受託運用者之一般義務以及將個人資料傳輸至第三國或國際組織。

Example 22: The Dutch consulate in Kingston, Jamaica, opens an online application process for the recruitment of local staff in order to support its administration.
示例 22：位在牙買加金斯敦的荷蘭領事館，為支援其行政管理，架設了一個在線申請流程，用於招聘當地員工。

While the Dutch consulate in Kingston, Jamaica, is not established in the Union, the fact that it is a consular post of an EU country where Member State law applies by virtue of public international law renders the GDPR applicable to its processing of personal data, as per Article 3(3).
雖然荷蘭牙買加金斯敦的領事館非設立於歐盟境內，但基於國際公法，該成員國之法律適用於國家之領事館，依據第 3 條第 3 項，領事館所為之個人資料運用屬於 GDPR 之適用範圍。

Example 23: A German cruise ship travelling in international waters is processing data of the guests on board for the purpose of tailoring the in-cruise entertainment offer.
示例 23：為提供客製化的郵輪娛樂項目，德國郵輪航行在國際水域時對船上客人進行資料運用。

While the ship is located outside the Union, in international waters, the fact that it is German- registered cruise ship means that by virtue of public international law the GDPR shall be applicable to its processing of personal data, as per Article 3(3).
雖然該郵輪非位於歐盟境內，然依據國際公法以及 GDPR 第 3 條第 3 項之規範，在德國註冊郵輪上所為之個人資料運用屬於 GDPR 之適用範圍。

Though not related to the application of Article 3(3), a different situation is the one where, by virtue of international law, certain entities, bodies or organisations established in the Union benefit from privileges and immunities such as those laid down in the Vienna Convention on Diplomatic Relations of 1961[27], the Vienna Convention on Consular Relations of 1963 or headquarter agreements concluded between international organisations and their host countries in the Union. In this regard, the EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic

[27] http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

missions and consular posts, as well as international organisations. At the same time, it is important to recall that any controller or processor that falls within the scope of the GDPR for a given processing activity and that exchanges personal data with such entities, bodies and organisations have to comply with the GDPR, including where applicable its rules on transfers to third countries or international organisations.
儘管與第 3 條第 3 項之適用無關，然另一種情況為，根據國際法，設立於歐盟境內之某些實體、機構或組織會受益於某些特權及豁免，諸如 1961 年之「維也納外交關係公約」[27]、1963 年之「維也納領事關係公約」或國際組織與歐盟成員國間締結之總部協定。於此情況下，EDPB 重申，GDPR 之適用並不影響國際法之規定，例如有關非歐盟外交使團和領事館以及國際組織特權及豁免之規定。同時，亦必須強調者為，任何屬於 GDPR 適用範圍之控管者或受託運用者，與上述實體、機構和組織就系爭運用活動交換個人資料時須遵守 GDPR，包括適用向第三國或國際組織傳輸資料之規則。

4. REPRESENTATIVE OF CONTROLLERS OR PROCESSORS NOT ESTABLISHED IN THE UNION
非設立於歐盟境內控管者或受託運用者之代表

Data controllers or processors subject to the GDPR as per its Article 3(2) are under the obligation to designate a representative in the Union. A controller or processor not established in the Union but subject to the GDPR failing to designate a representative in the Union would therefore be in breach of the Regulation.
依據第 3 條第 2 項，受 GDPR 管轄之資料控管者或受託運用者有義務於歐盟境內指定代表。未設立於歐盟境內但受拘束於 GDPR 之控管者或受託運用者，若未能於歐盟內指定代表，將違反 GDPR。

This provision is not entirely new since Directive 95/46/EC already provided for a similar obligation. Under the Directive, this provision concerned controllers not established on Community territory that, for purposes of processing personal data, made use of equipment, automated or otherwise, situated on the territory of a Member State. The GDPR imposes an obligation to designate a representative in the Union to any controller or processor falling under the scope of Article 3(2), unless they meet the exemption criteria as per Article 27(2). In order to facilitate the application of this specific provision, the EDPB deems it necessary to provide further guidance on the designation process, establishment obligations and responsibilities of the representative in the Union as per Article 27.
指令 95/46 / EC 亦有類似義務的規定。依據指令，該條款涉及未設立於歐盟境內之控管者，使用位於成員國領土內之自動化或其他設備運用個人資料。除符合第 27

條第 2 項之豁免標準外，任何屬於第 3 條第 2 項適用範圍內之控管者或受託運用者，GDPR 規定其有義務於歐盟境內指定代表。為便利執行此具體規範，EDPB 認為有必要依據第 27 條，就位於歐盟代表之指定程序、設立義務和責任提供進一步指導。

It is worth noting that a controller or processor not established in the Union who has designated in writing a representative in the Union, in accordance with article 27 of the GDPR, does not fall within the scope of article 3(1), meaning that the presence of the representative within the Union does not constitute an "establishment" of a controller or processor by virtue of article 3(1).
值得注意的是，依據 GDPR 第 27 條，非設立於歐盟境內之控管者或受託運用者在歐盟所指定之代表，不屬於第 3 條第 1 項之適用範圍。意即，依據第 3 條第 1 項，位於歐盟內之代表，並不構成控管者或受託運用者所設之「據點」。

a) Designation of a representative
a）指定代表

Recital 80 clarifies that "*[t]he representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation.*"
前言第 80 點闡明「*控管者或受託運用者應明確以書面委託代表履行其依照本規則所負之義務。該指定不影響控管者或受託運用者基於本規則所應負之責任或負擔。該代表應依據控管者或受託運用者之委託執行其任務，包括為確保符合本規則而需與主管機關合作之任何作為*」。

The written mandate referred to in Recital 80 shall therefore govern the relations and obligations between the representative in the Union and the data controller or processor established outside the Union, while not affecting the responsibility or liability of the controller or processor. The representative in the Union may be a natural or a legal person established in the Union able to represent a data controller or processor established outside the Union with regard to their respective obligations under the GDPR.
因此，前言第 80 點所提及之書面授權，規範位於歐盟境內之代表與位於歐盟外之

資料控管者或受託運用者間之關係和義務，且不影響控管者或受託運用者之責任或負擔。位於歐盟內之代表可以是在歐盟的自然人或法人，代表設立於歐盟外之資料控管者或受託運用者，履行其各自在 GDPR 下之義務。

In practice, the function of representative in the Union can be exercised based on a service contract concluded with an individual or an organisation, and can therefore be assumed by a wide range of commercial and non-commercial entities, such as law firms, consultancies, private companies, etc... provided that such entities are established in the Union. One representative can also act on behalf of several non-EU controllers and processors.
實務上，歐盟代表之運作可依據與個人或公司簽訂之服務契約行使，因此可以廣泛指定位於歐盟內之商業和非商業實體作為代表，例如律師事務所、諮詢公司和私人公司等。一個實體可同時代表數個非位於歐盟境內之控管者和受託運用者。

When the function of representative is assumed by a company or any other type of organisation, it is recommended that a single individual be assigned as a lead contact and person "in charge" for each controller or processor represented. It would generally also be useful to specify these points in the service contract.
當代表之運作由公司或任何其他類型組織執行時，建議應指派單一個人作為主要聯繫人，並為所代表之控管者或受託運用者「負責」。一般而言，於服務契約中載明這些重點是有用的。

In line with the GDPR, the EDPB confirms that, when several processing activities of a controller or processor fall within the scope of Article 3(2) GDPR (and none of the exceptions of Article 27(2) GDPR apply), that controller or processor is not expected to designate several representatives for each separate processing activity falling within the scope of article 3(2). The EDPB does not consider the function of representative in the Union as compatible with the role of an external data protection officer ("DPO") which would be established in the Union. Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers or processors are required to ensure that the DPO "*does not receive any instructions regarding the exercise of [his or her] tasks*". Recital 97 adds that DPOs, "*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*"[28]. Such requirement for a sufficient degree of autonomy and independence of a

[28] WP29 Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01.
WP29個資保護長指引，WP 243 rev.01。

data protection officer does not appear to be compatible with the function of representative in the Union. The representative is indeed subject to a mandate by a controller or processor and will be acting on its behalf and therefore under its direct instruction[29]. The representative is mandated by the controller or processor it represents, and therefore acting on its behalf in exercising its task, and such a role cannot be compatible with the carrying out of duties and tasks of the data protection officer in an independent manner.

為符合 GDPR，EDPB 確認，當控管者或受託運用者數項運用活動均屬於 GDPR 第 3 條第 2 項之適用範圍內（且 GDPR 第 27 條第 2 項之例外情況均不適用）時，該控管者或受託運用者不被期待就每一個屬於第 3 條第 2 項範圍內之單獨運用活動皆指派數位代表。EDPB 不認為歐盟代表的功能與設立於歐盟境內之外部個資保護長的作用一致。第 38 條第 3 項為確保個資保護長能在其組織內有足夠之自主權執行職務，規定了相關基本保障。尤其是要求控管者或受託運用者須確保個資保護長「*免於接受任何有關執行（其）任務之指示*」。前言第 97 點另補充，個資保護長「*無論是否受僱於控管者，都應該能以獨立方式執行其職責和任務*」[28]。個資保護長需具備足夠程度之自主權和獨立性的要件似乎與歐盟代表之功能不相符。歐盟代表確實需要控管者或受託運用者之授權，受其直接指示，代表其行事。[29] 該代表受其所代表之控管者或受託運用者之委託，因此代表其執行任務，而此種角色與以獨立方式履行職責和任務之個資保護長不相同。

Furthermore, and to complement its interpretation, the EDPB recalls the position already taken by the WP29 stressing that "*a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues*"[30].

此外，作為補充解釋，EDPB 檢視 WP29 所採行之立場，強調「*若在涉及資料保護案件中，要求個資保護長於法庭上代表控管者或受託運用者，則有利益衝突之可能*」[30]。

Similarly, given the possible conflict of obligation and interests in cases of enforcement proceedings, the EDPB does not consider the function of a data controller representative in the Union as compatible with the role of data processor for that same data controller, in particular when it comes to compliance with their respective responsibilities and compliance.

---

[29] An external DPO also acting as representative in the Union could for example be in a situation where he is instructed to communicate to a data subject a decision or measure taken by the controller or processor which he or she had deemed uncompliant with the provisions of the GDPR and advised against.
外部個資保護長同時作為歐盟代表時，可能發生一種情況，例如當個資保護長被指示向當事人傳達控管者或受託運用者的決定或措施時，該個資保護長反對並認為此決定或措施不符合GDPR之規範。

[30] WP29 Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01.
WP29個資保護長指引，WP 243 rev.01。

同樣地，鑑於在執法程序中可能存在之義務和利益衝突，EDPB 不認為，資料控管者位於歐盟境內之代表，其功能與隸屬同一資料控管者之資料受託運用者的角色相容。尤其是在遵守其各自之責任及合規性之面向上。

While the GDPR does not impose any obligation on the data controller or the representative itself to notify the designation of the latter to a supervisory authority, the EDPB recalls that, in accordance with Articles 13(1)a and 14(1)a, as part of their information obligations, controllers shall provide data subjects information as to the identity of their representative in the Union. This information shall for example be included in the [privacy notice and] upfront information provided to data subjects at the moment of data collection. A controller not established in the Union but falling under Article 3(2) and failing to inform data subjects who are in the Union of the identity of its representative would be in breach of its transparency obligations as per the GDPR. Such information should furthermore be easily accessible to supervisory authorities in order to facilitate the establishment of a contact for cooperation needs.
雖然 GDPR 並無施加義務予資料控管者或代表本身將其代表之身分通知監管機關，但 EDPB 引用第 13 條第 1 項 a 款和第 14 條第 1 項 a 款，認為依據控管者提供資訊之義務，控管者應提供當事人其歐盟代表之身分資訊。例如，該資訊應包含於資料蒐集時提供給當事人的[隱私聲明及]前置資訊中。非設立於歐盟境內但屬於第 3 條第 2 項適用範圍之控管者，若未向為當事人通知其代表人身分，將違反 GDPR 的透明義務。此外，監管機關應易於取得此類資訊，以便在合作需求上建立聯繫方式。

Example 24: The website referred to in example 12, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros or Sterling. The website indicates that photo albums can only be delivered by post mail in the France, Benelux countries and Germany. This website being subject to the GDPR, as per its Article 3(2)(a), the data controller must designate a representative in the Union.
示例 24：示例 12 提及之設立與管理皆位於土耳其的網站，為個性化家庭相冊的創建、編輯、印刷和運送提供服務。該網站提供英語、法語、荷蘭語和德語版本，且可用歐元或英鎊付款。 該網站表明，相冊只能通過郵寄方式在英國、法國、比荷盧聯盟國家和德國發送。該網站受 GDPR 約束，因此，依據第 3 條第 2 項 a 款，資料控管者必須在歐盟境內指定一名代表。

The representative must be established in one of the Member States where the service offered is available, in this case either in France, Belgium, Netherlands, Luxembourg or

Germany. The name and contact details of the data controller and its representative in the Union must be part of the information made available online to data subjects once they start using the service by creating their photo album. It must also appear in the website general privacy notice.
代表必須設立於服務提供所在地的成員國之一。在上述案例中，代表必須位於英國、法國、比利時、荷蘭、盧森堡或德國之其中一國。在當事人開始使用服務建立相冊時，資料控管者及其位於歐盟境內之代表的名稱和聯繫方式必須是線上資訊的一部分，且需註明於網站的一般隱私權聲明中。

b) Exemptions from the designation obligation[31]
b) 指定義務之免除 [31]

While the application of Article 3(2) triggers the obligation to designate a representative in the Union for controllers or processors established outside the Union, Article 27(2) foresees derogation from the mandatory designation of a representative in the Union, in two distinct cases:
雖然第3條第2項規定位於歐盟外之控管者或受託運用者需於歐盟境內指定代表，但第 27 條第 2 項列出在兩種不同的情況下，得克減該強制指定歐盟代表之義務：

- processing is "occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10", and such processing "is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing".
  資料運用係「偶然性之運用，不包括大規模運用第 9 條第 1 項所定之特殊類型個人資料或運用依第 10 條所定關於前科及犯罪之個人資料」，且「考量到運用之本質、過程、範圍與目的，不會對當事人之權利或自由造成風險者」。

In line with positions taken previously by the Article 29 Working Party, the EPDB considers that a processing activity can only be considered as "occasional" if it is not carried out regularly, and occurs outside the regular course of business or activity of the

[31] Part of the criteria and interpretation laid down in G29WP243 (Data Protection Officer) – endorsed by the EDPB can be used as a basis for the exemptions to the designation obligation.
由EDPB採認之G29WP243（個資保護長）中部分的標準和解釋可作為指定義務免除之基礎。

controller or processor[32].
依據 29 條工作小組先前之立場，EPDB 認為，運用活動只有在不定期執行且發生於控管者或受託運用者正常業務或活動範圍之外時，始可被視為「偶然」[32]。

Furthermore, while the GDPR does not define what constitutes large-scale processing, the WP29 has previously recommended in its guidelines WP243 on data protection officers (DPOs) that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned - either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity[33].
此外，雖然 GDPR 沒有定義大規模運用之構成要件，但 WP29 在關於個資保護長（DPOs）指引 WP243 中建議，為確認該行為是否為大規模運用時，應考慮下列要素：相關當事人的數量 – 特定數量或相對人口數比例；資料運用量/或運用不同資料項目的範圍；資料運用活動所持續之時間或永久性；運用活動的地域性[33]。

Finally, the EDPB highlights that the exemption from the designation obligation as per Article 27 refers to processing "unlikely to result in a risk to the rights and freedoms of natural persons"[34], thus not limiting the exemption to processing unlikely to result in a high risk to the rights and freedoms of data subjects. In line with Recital 75, when assessing the risk to the rights and freedom of data subjects, considerations should be given to both the likelihood and severity of the risk.
最後，EDPB 強調，第 27 條中對指定義務之免除係指「不太可能對自然人權利和自由造成風險」[34]之運用，因此，免除不僅限於對個資當事人權利和自由造成高風險之運用。依據前言第 75 點，在評估個資當事人權利和自由之風險時，應考量該風險之可能性和嚴重性。

[32] WP29 position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.
WP29關於GDPR第30條第5項的維護運用活動紀錄義務之例外的立場文件。
[33] WP 29 guidelines on data protections officers (DPOs), adopted on 13th December 2016, as last revised on 5th April 2017, WP 243 rev.01 – endorsed by the EDPB.
WP29個資保護長指引，2016年12月13日通過， 2017年4月5日最後修訂，WP 243 rev.01- 由EDPB採認 。
[34] Article 27(2)(a) GDPR.
GDPR第27條第2項第a款。

Or
或者

- processing is carried out "by a public authority or body".
  資料運用係由「公務機關或機構」執行。

The qualification as a "public authority or body" for an entity established outside the Union will need to be assessed by supervisory authorities *in concreto* and on a case by case basis.[35] The EDPB notes that, given the nature of their tasks and missions, cases where a public authority or body in a third country would be offering goods or services to data subject in the Union, or would monitor their behaviour taking place within the Union, are likely to be limited.
就成立於歐盟外之實體，其作為「公務機關或機構」之資格將需由監管機關*具體*評估，並視個案情況而定[35]。EDPB 指出，鑑於其作業和任務之性質，在某些情況下，當第三國之公務機關或機構向位於歐盟境內之個資當事人提供商品或服務，或監控其在歐盟境內之行為時，可能會受到限制。

c) Establishment in one of the Member States where the data subjects whose personal data are processed
c) 代表應設立於運用活動所涉及之當事人所在的成員國境內

Article 27(3) foresees that "the representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are". In cases where a significant proportion of data subjects whose personal data are processed are located in one particular Member State, the EDPB recommends, as a good practice, that the representative is established in that same Member State. However, the representative must remain easily accessible for data subjects in Member States where it is not established and where the services or goods are being offered or where the behaviour is being monitored.
第 27 條第 3 項規定「當運用活動涉及對當事人提供貨品或服務或監控其行為者，代表應設立於當事人所在之一成員國境內」。若運用活動所涉及之當事人大部分

[35] The GDPR does not define what constitutes a 'public authority or body'. The EDPB considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.
GDPR並無定義構成「公務機關或機構」之要件。EDPB認為，此一概念應依據國家法律加以確認。因此，公務機關和機構包括國家、地區和地方當局，但是依據所適用之國家法律，此概念通常亦包括一系列受公共法規管轄之其他機構。

位於某一特定成員國，作為良好的實踐，EDPB 建議代表應設立於該成員國境內。然而，若其他提供貨品或服務或監控行為之成員國未有指定代表，代表必須使該地之當事人可與之輕易取得聯繫。

The EDPB confirms that the criterion for the establishment of the representative in the Union is the location of data subjects whose personal data are being processed. The place of processing, even by a processor established in another Member State, is here not a relevant factor for determining the location of the establishment of the representative.

EDPB 確認，運用活動所涉及個資當事人的位置係設立歐盟代表之標準。至於該運用發生之地點則非決定代表設立地點之要素，即使該資料運用是由位於另一成員國境內之受託運用者所為。

Example 25: An Indian pharmaceutical company, with neither business presence nor establishment in the Union and subject to the GDPR as per Article 3(2), sponsors clinical trials carried out by investigators (hospitals) in Belgium, Luxembourg and the Netherlands. The majority of patients participating to the clinical trials are situated in Belgium.

示例 25：一家印度製藥公司，在歐盟境內沒有商業活動或設立據點，但贊助位於比利時、盧森堡和荷蘭調查員（醫院）所實行的臨床試驗，依第 3 條第 2 項之規定，屬於 GDPR 的適用範圍。大部分受試患者位於比利時。

The Indian pharmaceutical company, as a data controller, shall designate a representative in the Union established in one of the three Member States where patients, as data subjects, are participating to the clinical trial (Belgium, Luxembourg or the Netherlands). Since most patients are Belgian residents, it is recommended that the representative is established in Belgium. Should this be the case, the representative in Belgium should however be easily accessible to data subjects and supervisory authorities in the Netherlands and Luxembourg.

印度製藥公司作為資料控管者，應在病患（當事人）參與臨床試驗的三個成員國之一（比利時，盧森堡或荷蘭）指定歐盟代表。由於大多數病患為比利時居民，因此建議該代表應設立於比利時。於此情形，位於盧森堡或荷蘭的當事人和監管機關應可輕易地與位於比利時之代表聯繫。

In this specific case, the representative in the Union could be the legal representative of the sponsor in the Union, as per Article 74 of Regulation (EU) 536/2014 on clinical trials, provided that it does not act as a data processor on behalf of the clinical trial sponsor, that it is established in one of the three Member States, and that both functions are governed by and exercised in compliance with each legal framework.
在此特定案件中，依臨床試驗的規則（歐盟）536/2014 第 74 條，位於歐盟之代表可以是贊助商位於歐盟之法定代理人，然其不得作為資料受託運用者，代表臨床試驗贊助商，並須設立於三個成員國之一，且二者之功能皆須受拘束於且符合各自之法律架構。

d) Obligations and responsibilities of the representative
d）代表的義務及責任

The representative in the Union acts on behalf of the controller or processor it represents with regard to the controller or processor's obligations under the GDPR. This implies notably the obligations relating to the exercise of data subject rights, and in this regard and as already stated, the identity and contact details of the representative must be provided to data subjects in accordance with articles 13 and 14. While not itself responsible for complying with data subject rights, the representative must facilitate the communication between data subjects and the controller or processor represented, in order to make the exercise of data subjects' rights are effective.
位於歐盟的代表須代理履行資料控管者或受託運用者在 GDPR 下之義務，尤其是與當事人行使權利相關之義務。如上所述，需依據第 13 條和第 14 條，向當事人提供代表之身分和聯繫方式。代表雖不負維護當事人權利之責任，但必須促進當事人與其所代表之控管者或受託運用者間的溝通，以便當事人權利得有效實現。

As per Article 30, the controller or processor's representative shall in particular maintain a record of processing activities under the responsibility of the controller or processor. The EDPB considers that, while the maintenance of this record is an obligation imposed on both the controller or processer and the representative, the controller or processor not established in the Union is responsible for the primary content and update of the record and must simultaneously provide its representative with all accurate and updated information so that the record can also be kept and made available by the representative at all time. At the same time, it is the representative´s own responsibility to be able to provide it in line with Article 27, e.g. when being addressed by a

supervisory authority according to Art. 27(4).
依據第 30 條，就控管者或受託運用者所負責之運用活動，其代表應特別維護相關之活動記錄。EDPB 認為，當維護紀錄是控管者或受託運用者以及雙方代表之義務，非成立於歐盟境內之控管者或受託運用者負責主要內容並更新所有紀錄，且須同時提供其代表所有準確和更新之資訊，以便其隨時保留及提供活動紀錄。同時，代表有責任符合第 27 條之規定，例如依據第 27 條第 4 項，回應監管機構之要求。

As clarified by recital 80, the representative should also perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. In practice, this means that a supervisory authority would contact the representative in connection with any matter relating to the compliance obligations of a controller or processor established outside the Union, and the representative shall be able to facilitate any informational or procedural exchange between a requesting supervisory authority and a controller or processor established outside the Union.
如前言第 80 點所闡述，代表須依據控管者或受託運用者之委託執行其任務，包括為確保符合本規則而需與監管機關合作之任何作為。實際上，監管機關會就與非設立於歐盟內之控管者或受託運用者履行義務有關的任何事項聯繫其代表，且該代表應有能力促成監管機關與設立於歐盟境外之控管者或受託運用者間的任何資訊或程序交換。

With the help of a team if necessary, the representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication should in principle take place in the language or languages used by the supervisory authorities and the data subjects concerned or, should this result in a disproportionate effort, that other means and techniques shall be used by the representative in order to ensure the effectiveness of communication. The availability of a representative is therefore essential in order to ensure that data subjects and supervisory authorities will be able to establish contact easily with the non-EU controller or processor. In line with Recital 80 and Article 27(5), the designation of a representative in the Union does not affect the responsibility and liability of the controller or of the processor under the GDPR and shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves. The GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents in the Union.
必要時，在團隊合作下，歐盟代表必須能夠有效地與當事人進行溝通，並與相關

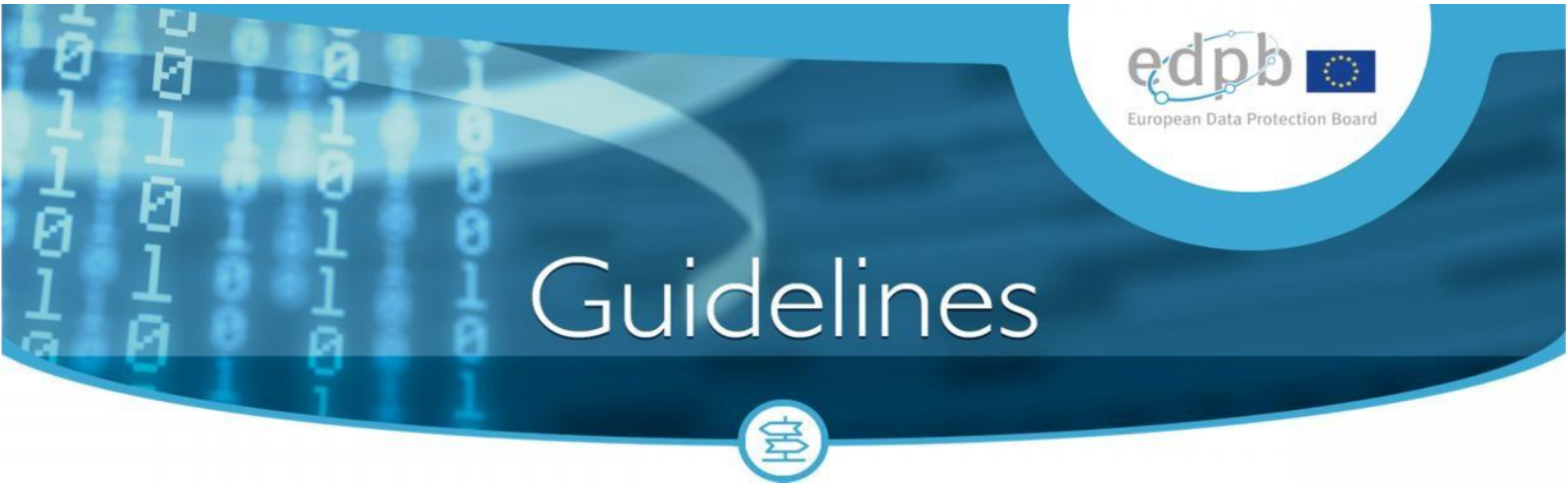
監管機關合作。這表示原則上該溝通所使用之語言，需與監管機關或個資當事人所使用之語言相同，或者，若如此會造成不符合比例原則之效能時，則該代表應使用其他方式和技術，以確保溝通之有效性。因此，代表的聯繫便利性對確保當事人和監管機關能夠與非設立於歐盟境內之控管者或受託運用者建立聯繫管道至關重要。依據前言第 80 點和第 27 條第 5 項，在歐盟中指定代表並不影響控管者或受託運用者在 GDPR 中應承擔的責任和義務，且應無礙於對該控管者或受託運用者本人提起訴訟。GDPR 並未就其在歐盟所代表之控管者或受託運用者建立代表之替代責任。

It should however be noted that the concept of the representative was introduced precisely with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. To this end, it was the intention to enable supervisory authorities to initiate enforcement proceedings through the representative designated by the controllers or processors not established in the Union. This includes the possibility for supervisory authorities to address corrective measures or administrative fines and penalties imposed on the controller or processor not established in the Union to the representative, in accordance with articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in articles 30 and article 58(1) a of the GDPR

另需指出，代表之概念被精確採用，係為了促進第 3 條第 2 項下之控管者或受託運用者之聯繫，並確保 GDPR 對其有效之執法。為此目的，代表之概念係為使監管機關能夠透過未成立於歐盟境內的控管者或受託運用者所指定之代表啟動執法程序。依據 GDPR 第 58 條第 2 項和第 83 條，此包括監管機關得透過施加糾正措施或行政罰鍰及懲罰於其代表，以懲處未成立於歐盟境內之控管者或受託運用者。然而，欲使代表負直接責任之可能性僅限於 GDPR 第 30 條和第 58 條第 1 項第 a 款所規範之直接義務。

The EDPB furthermore highlights that article 50 of the GDPR notably aims at facilitating the enforcement of legislation in relation to third countries and international organisation, and that the development of further international cooperation mechanisms in this regard is currently being considered.

EDPB 進一步強調，GDPR 第 50 條主要目的係促進與第三國和國際組織相關之法規執行，且目前正在考量此面向上可進一步發展之國際合作機制。



Guidelines 2/2018 on the derogations of Article 49 under Regulation 2016/679

關於第 2016/679 號規則(GDPR)第 49 條的例外情形之指引 2/2018

Adopted on 25 May 2018

2018 年 5 月 25 日通過

Contents 目錄

The European Data Protection Board

Having regard to Article 70 (1j) and (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED FOLLOWING GUIDELINES:

歐洲個人資料保護委員會

依據歐洲議會與歐盟理事會於 2016 年 4 月 27 日通過之歐盟 2016/679/EU 號規則（即 GDPR）第 70 條第 1 項第 j 款及第 e 款，有鑒於在運用（譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而 GDPR 對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將 GDPR 中的 processing 譯為「運用」，processor 譯為「受託運用者」）個人資料時對自然人之保護與確保該資料之自由流通，以及指令 95/46 / EC 之廢除，

通過以下指引：

1. GENERAL 總論

This document seeks to provide guidance as to the application of Article 49 of the General Data Protection Regulation (GDPR)[1] on derogations in the context of transfers of personal data to third countries.

本指引旨在就一般資料保護規則（GDPR）[1]第 49 條傳輸個人資料至第三國之例外情形提供指導。

The document builds on the previous work[2] done by the Working Party of EU Data Protection Authorities established under Article 29 of the Data Protection Directive (the WP29) which is taken over by the European Data Protection Board (EDPB) regarding central questions raised by the application of derogations in the context of transfers of personal data to third countries. This document will be reviewed and if

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016 年 4 月 27 日歐洲議會和歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，制定第 2016/679 號規則（EU），並廢除第 95/46 / EC 號指令（一般資料保護規則）。

necessary updated, based on the practical experience gained through the application of the GDPR.
本指引建立在依個人資料保護指令第29條所成立之歐盟第29條工作小組(WP29)（該小組由歐洲個人資料保護委員會（EDPB）取代）先前建構之基礎上[2]，適用於申請傳輸個人資料至第三國之例外情形。本文件將依據適用 GDPR 所得之實際經驗進行檢討，並在必要時更新。

When applying Article 49 one must bear in mind that according to Article 44 the data exporter transferring personal data to third countries or international organizations must also meet the conditions of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with.
在適用第 49 條時需注意，依據第 44 條，當資料輸出者將個人資料傳送至第三國或國際組織時，也必須符合 GDPR 其他條文之要件。每項運用活動必須符合相關資料保護規定，特別是有關第 5 條和第 6 條之規定。因此，須採行二步驟的分析方式：第一，資料運用的法源依據需符合 GDPR 所有相關條文規定；第二，需遵守第五章之規定。

Article 49 (1) states that in the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only under certain conditions. At the same time, Article 44 requires all provisions in Chapter V to be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. This also implies that recourse to the derogations of Article 49 should never lead to a situation where fundamental rights might be breached.[3]
第 49 條第 1 項規定，在沒有適足性認定或適當安全維護措施的情況下，一次傳輸或一系列傳輸個人資料至第三國或國際組織，需符合一定之要件。同時，第 44

[2] Article 29 Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, November 25,2005 (WP114).
29 條工作小組，依 1995 年 10 月 24 日第 95/46 / EC 號指令對第 26 條第 1 項所作共同解釋工作文件，2005 年 11 月 25 日（WP114）。

條要求適用第五章所有規定，需確保 GDPR 所保障之自然人保護程度不受減損。這也意味著訴諸第 49 條之例外情形不得導致可能違反基本權利之情事[3]。

The WP29, as predecessor of the EDPB, has long advocated as best practice a layered approach to transfers of considering first whether the third country provides an adequate level of protection and ensuring that the exported data will be safeguarded in the third country. If the level of protection is not adequate in light of all the circumstances, the data exporter should consider providing adequate safeguards. Hence, data exporters should first endeavor possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49 (1).

作為 EDPB 的前身，29 條工作小組長期以來一直主張以階層式方法評估傳輸為最佳實務做法[4]。首先需考量第三國是否可提供充足的保護，並確保被傳輸之資料在第三國得到保障。若在所有情況下，皆缺乏充足程度之保護時，資料輸出者應考量提供充分的安全維護措施。因此，資料輸出者應首先致力於依照 GDPR 第 45 條和第 46 條之機制來建構傳輸的可能性，且僅有在欠缺其要件的情形下，始可適用第 49 條第 1 項之例外情形。

Therefore, derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.[5] Due to this fact and in accordance with the principles inherent in European law,[6] the derogations must be interpreted restrictively so that the exception does not become the rule.[7] This is also supported by the wording of the title of Article 49 which states that derogations are to be used for specific situations ("Derogations for specific situations").

因此，第 49 條之例外情形係對一般原則之免除。一般原則係指個人資料之傳輸僅得發生在當第三國可提供充足程度之保護，或資料輸出者可提供適當安全維護措施，及當事人享有可執行且有效的權利，以便得以持續受益於其基本權利和保障。

[3] Article 29 Working Party, WP 114, p.9, and Article 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), p.39.
29 條工作小組，WP114，第 9 頁和 29 條工作小組有關為情報和國家安全目所為之監視電子通信工作文件（WP228），第 39 頁。

[4] Article 29 Working Party, WP114, p.9.
29 條工作小組，WP114，第 9 頁。

[5]依據此一事實與歐洲法律的既有原則[6]，例外情形須限縮解釋，才不致使例外成為規則。[7]第 49 條標題的用詞也支持此一論點，該條規定了例外適用的特定情形（「特定情形下之例外」）。

When considering transferring personal data to third countries or international organizations, data exporters should therefore favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data once this data has been transferred. As derogations do not provide adequate protection or appropriate safeguards for the personal data transferred and as transfers based on a derogation are not required to have any kind of prior authorisation from the supervisory authorities, transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned.

因此，在考量將個人資料傳輸到第三國或國際組織時，資料輸出者應該採行得為當事人提供保護之解決方式，即確保一旦資料被傳輸，當事人將繼續受益於其與資料運用相關之基本權利和保障。由於例外情形不能為傳輸之個人資料提供充足之保護或適當的安全維護措施，並且基於例外之傳輸不需要得到監管機關任何形式的事先授權，因此，依據例外情形將個人資料傳輸至第三國將導致當事人權利和自由的風險增加。

---

[5] Recital 114.
前言第 114 點。

[6] Article 29 Working Party, WP114, p.7.
29 條工作小組，WP114，第 7 頁。

[7] See already Article 29 Working Party, WP114, pg. 7. The European Court of Justice repeatedly underlined that "the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary" (judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C 73/07, paragraph 56; of 9 November 2010, Volker und Markus Schecke and Eifert, C 92/09 and C 93/09, paragraph 77; the Digital Rights judgment, paragraph 52, and of 6 October 2015, Schrems, C 362/14, paragraph 92, and of 21 December 2016, Tele2 Sverige AB, C 203/15, paragraph 96). See also report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2) (a), p.6 accessible at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.1)
請參照 29 條工作小組，WP114，第 7 頁。歐洲法院一再強調，「在歐盟體制下，基於保護尊重私生活的基本權利，個人資料保護之例外和限制僅在嚴格必要之情況始得適用」。（2008 年 12 月 16 日判決，SatakunnanMarkkinapörssi 和 Satamedia，C 73/07，第 56 段; 2010 年 11 月 9 日判決，Volker 和 Markus Schecke 和 Eifert，C 92/09 及 C 93/09，第 77 段; 數位權利判決第 52 段和 2015 年 10 月 6 日判決，Schrems，C 362/14，第 92 段；和 2016 年 12 月 21 日判決，Tele2 Sverige AB，C 203/15，第 96 段）。另請參照關於控管當局和跨境資訊傳輸第 108 號公約附加協議之報告，第 2 條第 2 項第 a 款，第 6 頁，可查閱 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.1）

Data exporters should also be aware that, in the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly limit transfers of specific categories of personal data to a third country or an international organization (Article 49 (5)).
資料輸出者另需注意，在無適足性認定的情況下，基於公共利益之重要原因，歐盟或其成員國的法律可明確限制特定類別個人資料傳輸至第三國或國際組織。（第 49 條第 5 項）。

Occasional and not repetitive transfers
非經常性且非重複性之傳輸

The EDPB notes that the term "occasional" is used in recital 111 and the term "not repetitive" is used in the "compelling legitimate interests" derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.
EDPB 指出，「非經常性」一詞用於前言第 111 點，「非重複性」一詞用於第 49 條第 1 項第 2 段例外情形下強調之「必要正當利益」。這些用詞表示此類傳輸雖可能不只發生一次，但非經常性，且需發生在常規的活動外，例如，在隨機、未知的情況下以及在任意的時間間隔內。例如，在資料輸出者和資料輸入者間的穩定關係中，定期發生之資料傳輸，基本上即可被視為是有系統且重複之傳輸行為，因此不得被當作是非經常性或非重複之傳輸。此外，當資料輸入者在通常情況下有權限直接存取資料庫（例如，透過 IT 應用程式之介面），資料之傳輸一般會被視為係經常性且反覆之行為。

Recital 111 differentiates among the derogations by expressly stating that the "contract" and the "legal claims" derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to "occasional" transfers, while such limitation is absent from the "explicit consent derogation", the "important reasons of public interest derogation", the "vital

interests derogation" and the "register derogation" pursuant to Article 49 (1) subpar. 1 (a), (d), (f) and, respectively, (g).
為區分例外情形，雖然前言第 111 點明確表示基於「契約」和「法律上主張」之例外（第 49 條第 1 項第 b、c 和 e 款）僅限於「非經常性」之傳輸，但「明確同意例外」、「公共利益重要原因例外」、「重大利益例外」和「登記例外」（第 49 條第 1 項第 a、d、f 和 g 款）皆無此類限制。

Nonetheless, it has to be highlighted that even those derogations which are not expressly limited to "occasional" or "not repetitive" transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.[8]
然而，仍須強調，即使上揭例外情形並未明確限於「非經常性」或「非重複性」之傳輸，此些條款仍須以不與例外本質矛盾之方式解釋，意即原則上不得將資料傳輸至第三國，除非該第三國對個人資料提供充足程度保護或以適當安全維護措施替代。[8]

Necessity test
必要性判斷

One overarching condition for the use of several derogations is that the data transfer has to be "necessary" for a certain purpose. The necessity test should be applied to assess the possible use of the derogations of Articles 49 (1) (b), (c), (d), (e) and (f). This test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used. For more information on the specific application of the necessity test in each of the concerned derogations, please refer to the relevant sections below.
數項引用例外情形之首要條件，係資料之傳輸就其特定目的而言是「必要」的。在評估第 49 條第 1 項第 b、c、d、e 及 f 款例外情形時，需考量必要性之要件。此要件要求位於歐盟之資料輸出者需評估，個人資料之傳輸對於為達到例外情形中之特殊目的是否為必要。有關必要性要件對每一例外情形之具體應用，請參閱以下相關章節。

[8] 原文即無文字呈現。

Article 48 in relation to derogations

第 48 條與例外情形之關聯

The GDPR introduces a new provision in Article 48 that needs to be taken into account when considering transfers of personal data. Article 48 and the corresponding recital 115 provide that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Therefore, a transfer in response to a decision from third country authorities is in any case only lawful, if in line with the conditions set out in Chapter V.[9]

在考慮傳輸個人資料時，需將 GDPR 在第 48 條中引入的新規定納入考量。第 48 條和相對應之前言第 115 點規定，第三國行政機關、法院或法庭之決定本身不得作為向該國傳輸資料的正當理由。因此，僅有在符合第五章之規定時，依據第三國機關決定而進行之傳輸始為合法。[9]

In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.

在有國際協定的情況下，例如司法互助協定（MLAT），歐盟公司通常應拒絕直接請求，並將現有的司法互助協定或其他協定介紹給請求之第三國機關。

This understanding also closely follows Article 44, which sets an overarching principle applying to all provisions of Chapter V, in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

上述理解也符合第 44 條之規範，該條設立了適用於第五章所有規定之總體原則，以確保不減損 GDPR 對自然人權利保障之程度。

[9] See Recital 115 sentence 4.
參照前言第 115 點，第 4 句。

2. SPECIFIC INTERPRETATION OF THE PROVISIONS OF ARTICLE 49
2. 第 49 條規定之具體解釋

2.1 The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards - Article (49 (1) (a))
2.1 第 49 條第 1 項第 a 款 – 當事人在被告知由於缺乏適足性認定和適當安全維護措施而導致資料傳輸對當事人可能造成的風險後，明確同意所計劃之傳輸

The general conditions for consent to be considered as valid are defined in Articles 4 (11)[10] and 7 of the GDPR[11]. The WP29 provides guidance on these general conditions for consent in a separate document, which is endorsed by the EDPB.[12] These conditions also apply to consent in the context of Article 49 (1) (a). However, there are specific, additional elements required for consent to be considered a valid legal ground for international data transfers to third countries and international organizations as provided for in Article 49 (1) (a), and this document will focus on them.
GDPR 第 4 條第 11 款[10]和第 7 條[11]對同意之定義被認為是有效之一般要件。29 條工作小組在另一份文件中提供對同意一般要件之指引，該文件已獲 EDPB 認可。[12] 此一般要件適用於第 49 條第 1 項第 a 款範圍內之同意。然而，依據第 49 條第 1 項第 a 款規定，若欲將同意作為向第三國和國際組織傳輸資料之有效法律依據，則尚需符合其他具體要件，本文件將側重於此些要件。

Therefore, this section (1) of the present guidelines shall be read in conjunction with the WP29 guidelines on consent, endorsed by the EDPB, which provide a more detailed analysis on the interpretation of the general conditions and criteria of consent under the GDPR.[13] It should also be noted that, according to Article 49 (3), public authorities are not able to rely on this derogation in the exercise of their public powers.
因此，本章節（1）應與 EDPB 所認可之 29 條工作小組的同意指引一併閱讀，該

[10] According to Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
依據 GDPR 第 4 條第 11 款，當事人之「同意」係指當事人為表達同意運用與其有關之個人資料，藉由聲明或清楚肯定之行動而自由給予之特定、知情及非模糊之意思表示。
[11] Also recitals 32, 33, 42 and 43 give further guidance on consent.
有關同意之進一步闡釋，請參照前言第 32 點、33 點、42 點和 43 點。
[12] See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259).
參照 29 條工作小組依據第 2016/679 號規則簽署之同意指引（WP259）。

文件對 GDPR 中同意的一般要件和標準的解釋，提供了更詳細的分析。[13] 另需注意，依據第 49 條第 3 項，公務機關在行使其公權力時不適用此例外規定。

Article 49 (1) (a) states that a transfer of personal data to a third country or an international organization may be made in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, on the condition that 'the data subject has *explicitly consented* to the proposed transfer, *after having been informed of the possible risks* of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards'.

第 49 條第 1 項第 a 款規定，於欠缺第 45 條第 3 項之適足性認定，或欠缺第 46 條之適當安全維護措施時，包括有拘束力之企業守則，傳輸個人資料至第三國或國際組織需符合「當當事人*已被告知*因欠缺適足性認定及適當安全維護措施*可能對自身造成之風險後*，已*明確同意*所計劃之傳輸」。

2.1.1 Consent must be explicit
2.1.1 同意必須明確

According to Article 4 (11) of the GDPR, any consent should be freely given, specific, informed and unambiguous. On this very last condition, Article 49 (1) (a) is stricter as it requires "explicit" consent. This is also a new requirement in comparison to Article 26 (1) (a) of Directive 95/46/EC, which only required "unambiguous" consent. The GDPR requires explicit consent in situations where particular data protection risks may emerge, and so, a high individual level of control over personal data is required, as is the case for the processing of special category data (Article 9 (2) (a)) and automated decisions (Article 22 (2) (c)). Such particular risks also appear in the context of international data transfers.

依據 GDPR 第 4 條第 11 款之規定，任何同意都應該是自由給予、特定的、知情的和非模糊的。在最後一個要件下，第 49 條第 1 項第 a 款規定更為嚴格，因為該條要求同意必須「明確」。與指令 95/46 / EC 第 26 條第 1 項第 a 款相較，明確同意亦是一項新要求，因該指令僅要求同意需「不模糊」。GDPR 要求在可能出現特殊資料保護風險，因而需要對個人資料有更高度之個別控制水平時，同意必須

[13] Idem.
同上。

明確，例如在運用特殊類別資料（第 9 條第 2 項第 a 款）和自動化決策（第 22 條第 2 項第 c 款）的情形。此種特殊風險也存在於國際資料傳輸的情形。

For further guidance on the requirement of explicit consent, and for the other applicable requirements needed for consent to be considered valid, please refer to the WP29's Guidelines on Consent which are endorsed by the EDPB.[14]
有關明確同意要求的進一步指導，以及有效同意所需要的其他適用要求，請參閱由 EDPB 認可之 29 條工作小組的同意指引。[14]

2.1.2 Consent must be specific for the particular data transfer/set of transfers
2.1.2 針對特定資料傳輸/系列傳輸需給予明確同意

One of the requirements of valid consent is that it must be specific. In order to constitute a valid ground for a data transfer pursuant to Article 49 (1) (a), hence, consent needs to be specifically given for the particular data transfer or set of transfers.
同意必須特定係有效同意的要件之一。 因此，為構成第 49 條第 1 項第 a 款進行資料傳輸的有效理由，針對特定的資料傳輸或系列傳輸，必須提供明確的同意。

The element "specific" in the definition of consent intends to ensure a degree of user control and transparency for the data subject. This element is also closely linked with the requirement that consent should be "informed".
同意定義中的「特定」要件旨在確保當事人一定程度的用戶控制權和透明化。此要件與同意中「知情」之要求密切相關。

Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed. As an example, an EU company collects its customers' data for a specific purpose (delivery of goods) without considering transferring this data, at that time, to a third party outside the EU. However, some years later, the same company is acquired by a non-EU company which wishes to transfer the personal data of its customers to another company outside the EU. In order for this transfer to be valid on the grounds of the consent derogation, the data subject should give his/her consent for this specific transfer at the time when the transfer is

[14] Idem.
同上。

envisaged. Therefore, the consent provided at the time of the collection of the data by the EU company for delivery purposes is not sufficient to justify the use of this derogation for the transfer of the personal data outside the EU which is envisaged later.
由於同意必須特定，因此有時無法在蒐集資料時獲得當事人事先同意將來的傳輸，例如，若在要求同意時無法明確知悉傳輸的發生和具體情況，則無法評估對當事人的影響。例如，歐盟公司為特定目的（交付貨品）蒐集客戶資料時，並未考慮將此資料傳輸至歐盟以外之第三國。然而，幾年後，同一家公司被一家非歐盟公司收購，該公司希望將其客戶的個人資料傳輸至歐盟以外的另一家公司。為使該傳輸符合同意之例外情形而為有效，當事人須對預期之特定傳輸表示同意。因此，當事人因貨品交付而同意歐盟公司對其個資之蒐集，不足以合理化其基於例外而事後傳輸個人資料至歐盟境外之情形。

Therefore, the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made. This requirement is also related to the necessity for consent to be informed. It is possible to obtain the specific consent of a data subject prior to the transfer and at the time of the collection of the personal data as long as this specific transfer is made known to the data subject and the circumstances of the transfer do not change after the specific consent has been given by the data subject. Therefore the data exporter must make sure that the requirements set out in section 1.3 below are also complied with.
因此，資料輸出者必須確保在傳輸前獲得當事人對傳輸的特定同意，即使該傳輸發生在資料蒐集之後。此項要求與同意中知情的必要性相關。只要當事人知悉該特定傳輸且傳輸的情況在當事人為特定同意後並無改變，即有可能在資料傳輸之前和蒐集個人資料時獲得當事人對傳輸之特定同意。因此，資料輸出者必須亦確保符合以下第 1.3 節中規定之要求。

2.1.3 Consent must be informed[15] particularly as to the possible risks of the transfer
2.1.3 同意必須為知情的[15]，尤其是關於傳輸可能造成之風險

This condition is particularly important since it reinforces and further specifies the general requirement of "informed" consent as applicable to any consent and laid down in Art. 4 (11).[16] As such, the general requirement of "informed" consent, requires, in

[15] The general transparency requirements of Articles 13 and 14 of the GDPR should also be complied with. For more information see Guidelines on transparency under Regulation 2016/679 (WP 260).
亦須遵守 GDPR 第 13 條和第 14 條的一般透明化要求。更多資訊請參閱第 2016/679 號規則透明化指引（WP 260）。

the case of consent as a lawful basis pursuant to Article 6(1) (a) for a data transfer, that the data subject is properly informed in advance of the specific circumstances of the transfer, (i.e. the data controller's identity, the purpose of the transfer, the type of data, the existence of the right to withdraw consent, the identity or the categories of recipients).[17]

此要件之重要性在於其強化並進一步說明了適用於第4條第11款同意的一般要求中，規範任何同意必須為「知情」的同意。[16] 因此，「知情」同意的一般要求，在依據第 6 條第 1 項第 a 款以同意作為進行資料傳輸的合法基礎情況下，要求當事人在特定傳輸情況之前獲得適當的通知（即資料控管者之身分、傳輸之目的、資料的類型、撤回同意的權利以及資料接收者之身分或類別）。[17]

In addition to this general requirement of "informed" consent, where personal data are transferred to a third country under Article 49 (1) (a), this provision requires data subjects to be also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented. The provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer and therefore if it is not supplied, the derogation will not apply.

除了「知情」同意的一般要求外，依據第 49 條第 1 項第 a 款規定將個人資料傳輸至第三國，當該第三國無法對個人資料提供充足保護且無針對傳輸資料提供適當安全維護措施時，該條款要求當事人應被告知該傳輸之具體風險。為了使當事人在完全了解傳輸的具體事實下行使其同意，此資訊中之條款至關重要，因此，若無法提供此資訊，則例外情形不適用。

The information provided to data subjects in order to obtain consent for the transfer of their personal data to third parties established in third countries should also specify all data recipients or categories of recipients, all countries to which the personal data are being transferred to, that the consent is the lawful ground for the transfer, and that the third country to which the data will be transferred does not provide for an adequate level of data protection based on a European Commission decision.[18] In addition, as mentioned above, information has to be given as to the possible risks for the data

[16] See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259).
請參閱 29 條工作小組第 2016/679 號規則同意指引（WP 259）。
[17] Idem, page 13
同上，第 13 頁。

subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards. Such notice, which could be standardized, should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country.
為了獲得當事人同意將個人資料傳輸至設立於第三國之第三方而提供之資訊，應詳細指明所有資料接收者或接收者之類別、所有個人資料擬傳輸之國家、同意是傳輸的合法依據、以及資料傳輸至之第三國並未根據歐盟執委會的決議提供充足程度的資料保護。[18]此外，如上所述，資訊亦須包含有關當事人因第三國缺乏充足保護以及缺乏適當安全維護措施而可能存在之風險。此類可被標準化之通知應包括例如在該第三國可能沒有監管機關、和/或資料運用原則、和/或第三國可能無法提供當事人權利等資訊。

In the specific case where a transfer is performed after the collection of personal data from the data subject has been made, the data exporter should inform the data subject of the transfer and of its risks before it takes place so as to collect his explicit consent to the "proposed" transfer.
在從當事人蒐集個人資料後始進行傳輸的特定情形下，資料輸出者應在資料傳輸發生前告知當事人該傳輸及風險，並獲得其對此「計劃」之傳輸明確的同意。

As shown by the analysis above, the GDPR sets a high threshold for the use the derogation of consent. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long term solution for transfers to third countries.
如上所示，GDPR 對例外情形下之同意設立很高的門檻。此一高門檻，再加上當事人可隨時撤回其同意之事實，意味著同意可能不是傳輸資料至第三國之可行長期解決方案。

2.2 Transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken at the data subject's request – (49(1)(b))
2.2 第 49 條第 1 項第 b 款 – 傳輸對履行當事人與控管者間契約、或依當事人之請求執行契約前措施為必要

[18] The last mentioned requirement also stems from the duty to inform the data subjects (Article 13(1)(f), Article 14(1)(e)).
最後提及之要件亦源於向當事人提供資訊之義務(第 13 條第 1 項第 f 款和第 14 條第 1 項第 e 款)。

In view of recital 111, data transfers on the grounds of this derogation may take place "where the transfer is ***occasional*** and ***necessary*** in relation to a contract (...)"[19]
依據前言第 111 點，基於這種例外之資料傳輸可能發生在當「傳輸***非經常性***且基於契約有所***必要***（.....）」。[19]

In general, although the derogations relating to the performance of a contract may appear to be potentially rather broad, they are being limited by the criterions of "*necessity*" and of "*occasional transfers*".
一般而言，雖然與履行契約相關之例外情形似乎相當廣泛，但仍受到「*必要性*」和「*非經常性傳輸*」之標準限制。

Necessity of the data transfer
資料傳輸之必要性

The "*necessity test*"[20] limits the number of cases in which recourse can be made to Article 49 (1) (b).[21] It requires a close and substantial connection between the data transfer and the purposes of the contract.
「*必要性判斷*」[20] 限制了可訴諸第 49 條第 1 項第 b 款的案件數量。[21] 該條款要求資料傳輸與契約目的之間存在密切且實質的關聯。

This derogation cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer.[22] Other grounds for transfer as provided for in Chapter V such as standard contractual clauses or binding corporate rules may, however, be suitable for the particular transfer.
例如，當企業集團為了營業目的而將所有員工的(薪資)給付和人力資源管理的功能集中於第三國處理時，即不適用此類型之例外情形，因為僱傭契約的履行與資

[19] The criterion of "occasional" transfers is found in recital 111 and applies to the derogations of Article 49 (1) (b), (c) and (e).
「非經常性」移轉之標準見於前言第 111 點，並適用於第 49 條第 1 項第 b、c 和 e 款之例外情形。
[20] See also Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217).
請另參閱 29 條工作小組意見 06/2014，有關資料控管者依據指令 95/46 / EC（WP 217）第 7 條的正當利益概念。
[21] The "necessity" requirement also can be found in the derogations set forth in Article 49 (1) (c) to (f).
「必要性」要求亦規範於第 49 條第 1 項第 c 至 f 款之例外情形。

料傳輸之間並無直接和客觀的關聯。[22] 然而，第五章規定的其他傳輸理由，如標準契約條款或具有約束力的企業守則，則可適用於此特定傳輸。

On the other hand, the transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would be called upon in the organization of these clients' stay abroad can be deemed necessary for the purposes of the contract entered into by the travel agent and the client, since, in this case, there is a sufficient close and substantial connection between the data transfer and the purposes of the contract (organization of clients' travel).
另一方面，旅遊業者為安排其客戶在國外旅行，將有關客戶的個人資料傳輸至酒店或其他可能拜會的商業合作夥伴，此傳輸行為可被視為履行旅遊業者和客戶間之契約所必須，因為在此種情形下，資料傳輸與契約目的（客戶旅遊的安排）之間存在足夠密切且實質的關聯。

This derogation cannot be applied to transfers of additional information not necessary for the performance of the contract or, respectively, for the implementation of precontractual measures requested by the data subject[23]; for additional data other tools would hence be required.
此類型之例外不得適用於傳輸其他非履行契約以及執行當事人要求之契約前行為所必要之額外資訊[23]；傳輸額外資料尚需其他方法。

Occasional transfers
非經常性之傳輸

Personal data may only be transferred under this derogation when this transfer is occasional.[24] It would have to be established on a case by case basis whether data transfers or a data transfer would be determined as "*occasional*" or "*non-occasional*".
個人資料僅有在非經常性之傳輸時始有例外情形的適用。[24]必須依據具體個案情況認定資料之傳輸或系列傳輸是否可被視為係「*非經常性*」或「*經常性*」。

[22] In addition it will not be seen as being occasional (see below).
此外，該移轉行為不會被視為係非經常性之移轉（見下文）。
[23] More generally, all derogations of Article 49(1) (b) to (f) only allow that the data which are necessary for the purpose of the transfer may be transferred.
更一般地說，第 49 條第 1 項第 b 至 f 款的所有例外情形僅適用於當移轉係為實現其目的所必要時始可為之。
[24] As to the general definition of the term « occasional » see page 4.
「非經常性」的一般定義請參見第 4 頁(譯註：即本翻譯文件第 8 頁)。

A transfer here may be deemed occasional for example if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings. A transfer could also be considered as occasional if a bank in the EU transfers personal data to a bank in a third country in order to execute a client's request for making a payment, as long as this transfer does not occur in the framework of a stable cooperation relationship between the two banks.
例如，某一銷售經理基於僱傭契約需拜訪位於第三國的不同客戶時，此處的傳輸該經理個人資料給客戶以便安排會議即可被視為非經常性。若位於歐盟的銀行將個人資料傳輸至第三國的銀行以執行客戶的付款請求，只要該傳輸不屬於兩家銀行之間穩定合作關係的框架內，即可被視為係非經常性之傳輸。

On the contrary, transfers would not qualify as "occasional" in a case where a multi-national company organises trainings in a training centre in a third country and systematically transfers the personal data of those employees that attend a training course (e.g. data such as name and job title, but potentially also dietary requirements or mobility restrictions). Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "occasional" character. Consequently, in this case many data transfers within a business relationship may not be based on Article 49 (1) (b).
相反的，若跨國公司在第三國的培訓中心安排培訓，並有系統地傳輸參加培訓課程員工的個人資料（例如，姓名和職稱等，亦可能是對飲食要求或行動限制的資料），該傳輸則不符合「非經常性」之要件。在穩定關係中定期發生的資料傳輸應被視為是系統性且重複的行為，故而超出了「非經常性」的定義。因此，於此情形下，業務關係中之許多資料傳輸不屬於第 49 條第 1 項第 b 款之適用範圍。

According to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.
依據第 49 條第 1 項及第 3 項，此例外情形不適用於公務機關執行公權力之活動。

2.3 Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person - (49 (1) (c))

2.3 第 49 條第 1 項第 c 款 – 傳輸對締結或履行控管者與其他自然人或法人間，基於當事人之利益所締結之契約為必要

The interpretation of this provision is necessarily similar to that of Article 49 (1) (b); namely, that a transfer of data to a third country or an international organization in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, can only be deemed to fall under the derogation of Article 49(1) (c), if it can be considered to be "*necessary for the conclusion or performance of a contract between the data controller and another natural or legal person, in the interest of the data subject*".

此條款之解釋應類似於第 49 條第 1 項第 b 款之解釋；也就是在欠缺第 45 條第 3 項之適足性認定時，或欠缺第 46 條之適當安全維護措施時，若欲適用第 49 條第 1 項第 c 款之例外情形，將個人資料傳輸至第三國或國際組織須符合「*傳輸對締結或履行控管者與其他自然人或法人間，基於當事人之利益所締結之契約為必要*」。

Aside from being necessary, recital 111 indicates that, data transfers may only take place "*where the transfer is **occasional** and **necessary** in relation to a contract (...)*" Therefore, apart from the "*necessity test*", personal data here as well may only be transferred under this derogation only when the transfer is occasional.

除了必要之要件外，前言第 111 點指出，資料之傳輸僅可發生於「*當傳輸基於契約上主張之**必要**而**非經常性**之情形*（.....）」。因此，除了「*必要性判斷*」外，此處之資料傳輸也僅有在該傳輸係非經常性時始可適用例外情形。

Necessity of the data transfer and conclusion of the contract in the interest of the data subject

資料傳輸和契約締結係基於當事人利益之必要

Where an organization has, for business purposes, outsourced activities such as payroll management to service providers outside the EU, this derogation will not provide a basis for data transfers for such purposes, since no close and substantial link between the transfer and a contract concluded in the data subject's interest can be established even if the end purpose of the transfer is the management of the pay of the employee.[25] Other transfer tools provided in Chapter V may provide a more suitable basis for such transfers such as standard contractual clauses or binding corporate rules.

若公司基於商業目的，將諸如薪資管理等活動外包給位於歐盟外之服務提供者，即使傳輸的最終目的係管理員工薪資，例外情形之規範仍無法作為此類型傳輸之依據，因為該傳輸與基於當事人之利益而締結的契約之間沒有密切和實質性之關

聯。[25]第五章規定的其他傳輸方法，如標準契約條款或具有拘束力之企業守則，可為此類型之傳輸提供更適合之基礎。

Occasional transfers

非經常性之傳輸

Moreover, personal data may only be transferred under this derogation, when the transfer is occasional as it is the case under the derogation of Article 49 (1) (b). Therefore, in order to assess whether such transfer is occasional, the same test has to be carried out[26].

此外，如同第 49 條第 1 項第 b 款的例外情形，此處之例外僅適用於當個人資料之傳輸屬非經常性。因此，為評估該傳輸是否屬非經常性，須適用相同之標準進行評估。[26]

Finally, according to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.[27]

最後，依據第 49 條第 1 項及第 3 項，此例外情形不適用於公務機關執行公權力之活動。[27]

2.4 Transfer is necessary for important reasons of public interest - (49 (1) (d))

2.4 第 49 條第 1 項第 d 款 – 傳輸因公共利益之重要原因為必要

This derogation, usually referred to as the "important public interest derogation", is very similar to the provision contained in Directive 95/46/EC[28] under Article 26 (1) (d), which provides that a transfer shall take place only where it is necessary or legally required on important public interest grounds.

這類型之例外情形，通常被稱作「重要公共利益之例外」。與指令 95/46 / EC 第 26 條第 1 項第 d 款[28]的規定非常相似，該條款規定傳輸之發生僅可基於必要或法律上所要求之重要公共利益。

---

[25] In addition it will not be seen as being occasional (see below).
此外，該移轉行為不會被視為係非經常性之移轉（見下文）。

[26] As to the general definition of the term "occasional" please see page 4.
「非經常性」之一般定義請參見第 4 頁(譯註：即本翻譯文件第 8 頁)。

[27] For more information please refer to section 1, page 5 above.
詳細資訊請參閱前述第一節，第 5 頁(譯註：即本翻譯文件第 9 頁)。

[28] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

According to Article 49 (4), only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.
依據第 49 條第 4 項，只有在歐盟法或控管者受拘束之成員國法所承認之公共利益才適用於此例外情形。

However, for the application of this derogation, it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law. Where for example a third country authority requires a data transfer for an investigation aimed at combatting terrorism, the mere existence of EU or member state legislation also aimed at combatting terrorism is not as such a sufficient trigger to apply Article 49 (1) (d) to such transfer. Rather, as emphasized by the WP29, predecessor of the EDPB, in previous statements,[29] the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest pursuant to Article 49 (1) (d), as long as the EU or the Member States are a party to that agreement or convention.
然而，在此例外情形實際適用上，當第三國為其公共利益進行調查，而要求資料傳輸（例如由第三國主管機關），即使在抽象概念層面，此公共利益也存在於歐盟或成員國法律中，該要求仍不足以符合例外的情形。例如，第三國政府為打擊恐怖主義的調查要求資料傳輸，即使歐盟或成員國的法律亦存在打擊恐怖主義的相關規範，該立法並不足以觸發第 49 條第 1 項第 d 款之適用。相反的，正如 EDPB 的前身 29 條工作小組在先前陳述中所強調的[29]，只有在歐盟法律或控管者所受拘束之成員國法律所承認可被用於作為資料傳輸之重要公共利益目的者，包括基於互惠精神而進行的國際合作，始有例外情形之適用。依據第 49 條第 1 項第 d 款評估公共利益之存在與否時，現有之國際協定或公約只要其認可某一目標並提供國

1995 年 10 月 24 日歐洲議會和理事會通過之第 95/46 / EC 號指令，關於保護自然人之個人資料運用和該資料之自由流通。

[29] Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), p. 25.
29 條工作小組有關環球同業銀行金融電信協會（SWIFT）運用個人資料第 10/2006 號意見（WP128），第 25 頁。

際合作以促成該目標，則該國際協定或公約可作為衡量標準，只要歐盟或其成員國是該協議或公約的締約方。

Although mainly focused to be used by public authorities, Article 49 (1) (d) may also be relied upon by private entities. This is supported by some of the examples enumerated in recital 112 which mention both transfers by public authorities and private entities[30].
雖然主要著重於公務機關之援用，但私人實體亦適用第49條第1項第d款之規範。前言第112點中所列舉之範例可作為依據，該前言中提及了公務機關和私人實體所為之傳輸[30]。

As such, the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organization (public, private or international organization) that transfers and/or receives the data.
因此，適用此類例外的基本要求係找到重要公共利益為何，而非傳輸和/或接收資料組織（公共、私人或國際組織）之性質。

Recitals 111 and 112 indicate that this derogation is not limited to data transfers that are "occasional"[31]. Yet, this does not mean that data transfers on the basis of the important public interest derogation under Article 49 (1) (d) can take place on a large scale and in a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 shall not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.[32]
前言第111點和第112點指出此類例外情形之適用不限於「非經常性」[31] 的資料傳輸。然而，這並不意味著可基於第49條第1項第d款重大公共利益之例外而進行大規模和系統性的資料傳輸。相反的，仍需遵守一般性原則。依據該原則，第

[30] "international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport."
「例如競爭法主管機關、稅務或關務機關之間、金融監管機關之間、社會安全或公共衛生服務專責機關之間的國際資料交換；例如傳染病之接觸追蹤或為了降低並/或消除運動比賽興奮劑濫用之情形」。
[31] As to the general definition of the term « occasional » see page 4.
「非經常性」的一般定義請參見第4頁(譯註：即本翻譯文件第8頁)。

49 條規範之例外情形不得在實踐中被視為「規則」，而必須被限縮至特定情形，且各資料輸出者須確保傳輸符合嚴格的必要性判斷。[32]

Where transfers are made in the usual course of business or practice, the EDPB strongly encourages all data exporters (in particular public bodies[33]) to frame these by putting in place appropriate safeguards in accordance with Article 46 rather than relying on the derogation as per Article 49(1) (d).
若因通常的商業行為或業務而進行之傳輸，EDPB 強烈建議所有資料輸出者（特別是公務機關[33]）依據第 46 條制定適當的安全維護措施，而非依賴第 49 條第 1 項第 d 款的例外情形。

2.5 Transfer is necessary for the establishment, exercise or defense of legal claims - (49 (1) (e))
2.5 第 49 條第 1 項第 e 款 – 傳輸對建構、行使或防禦法律上之請求為必要

Establishment, exercise or defense of legal claims
建構、行使或防禦法律上之請求

Under Article 49 (1) (e), transfers may take place when "*the transfer is necessary for the establishment, exercise or defense of legal claims*". Recital 111 states that a transfer can be made where it is "*occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies*". This covers a range of activities for example, in the context of a criminal or administrative investigation in a third country (e.g. anti-trust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen e.g. in anti-trust investigations. As well, data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation. It can also cover actions by the data exporter to institute procedures in a third country for example commencing litigation or seeking approval for a merger. The derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that

[32] See also page 3.
另參見第 3 頁(譯註：即本翻譯文件第 4 頁)。
[33] For example financial supervisory authorities exchanging data in the context of international transfers of personal data for administrative cooperation purposes.
例如，金融監管機關為了行政合作目的，在國際個資移轉的背景下交換資料。

legal proceedings or formal procedures may be brought in the future.
第 49 條第 1 項第 e 款規定，當「*傳輸對建構、行使或防禦法律上之請求為必要*」時可進行傳輸。前言第 111 點指出，傳輸須「*基於契約或法律上主張之必要且不具經常性，不問係基於訴訟、行政程序或任何法庭外程序，包括監管機關前之程序*」。此涵蓋了一系列程序，例如，在第三國的刑事或行政調查中（例如反壟斷法、貪腐、內線交易或其他類似情況），為自身之辯護或為減輕或免除法律上可預見罰鍰之目的（例如在反壟斷調查案件），資料之傳輸可適用例外情形。同樣，在民事訴訟程序中，因正式的審前證據開示程序而進行之資料傳輸亦可適用於例外情形。這也包含資料輸出者在第三國所發動之程序行為，例如提起訴訟或申請合併批准。然而，僅僅只是未來有可能提起法律訴訟或正式程序，不得作為例外情形下傳輸資料之正當理由。

This derogation can apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).
此例外情形可適用於公務機關執行公權力之活動（第 49 條第 3 項）。

The combination of the terms “legal claim” and “procedure” implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures (“or any out of court procedure”). As a transfer needs to be made in a procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient.
「法律上之請求」和「程序」的合併使用意味著相關程序必須具有法律依據，包括正式、依法定義之程序，但不限於司法或行政程序（「或任何法庭外程序」）。由於傳輸須發生於程序進行中，因此資料傳輸和系爭情況下之特定程序間應有密切之關聯。對某種程序的抽象適用性不足以符合該條之要件。

Data controllers and data processors need to be aware that national law may also contain so-called “blocking statutes”, prohibiting them from or restricting them in transferring personal data to foreign courts or possibly other foreign official bodies.
資料控管者和資料受託運用者需清楚意識到，國家法律也可能包含所謂的「阻礙性法律」（blocking statutes），禁止或限制將個人資料傳輸至外國法院或其他可能之外國官方機構。

Necessity of the data transfer

資料傳輸之必要性

A data transfer in question may only take place when it is necessary for the establishment, exercise or defense of the legal claim in question. This "*necessity test*" requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position.[34] The mere interest of third country authorities or possible "good will" to be obtained from the third country authority as such would not be sufficient.

資料之傳輸只有對建構、行使或防禦法律上之請求為必要時始得為之。此「*必要性判斷*」要求所涉及之資料與建構、行使或防禦法律上之請求之間存在密切且實質之關聯。[34] 僅係基於第三國當局之利益或從第三國當局可能獲得之「善意」不足以符合必要性之要件。

Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

雖然資料輸出者為回覆請求或提起訴訟程序，有誘因傳輸所有可能相關的個人資料，然而，此行為不符合例外情形和 GDPR 之一般適用，因為 GDPR 強調（基於資料最小化原則）個人資料必須適當、相關且限於運用之目的所必要。

In relation to litigation proceedings the WP29, predecessor of the EDPB, has already set out a layered approach to the question of whether the personal data should be transferred, including the application of this principle. As a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer – so only a set of personal data that is actually necessary is transferred and disclosed.

關於訴訟程序，EDPB 的前身 29 條工作小組已就是否得傳輸個人資料的問題制定

[34] Recital 111: "necessary in relation to a contract or a legal claim."
前言第 111 點：「基於契約或法律上主張之必要。」

了階層式的分析方法，該分析方法亦適用於此原則。第一步，應仔細評估匿名資料在特定情況下是否足夠。若不足夠，則可考慮傳輸假名化資料（pseudonymized data）。若將個人資料傳輸至第三國為必要時，則應在傳輸前評估其與特定事實之關聯性 - 因此，只需傳輸和揭露實際所需之個人資料。

Occasional transfer

非經常性之傳輸

Such transfers should only be made if they are occasional. For information on the definition of occasional transfers please see the relevant section on "occasional and "non-repetitive" transfers.[35] Data exporters would need to carefully assess each specific case.

此類型之傳輸僅得於非經常性的情況下始得為之。有關非經常性傳輸之定義，請參閱「非經常性」和「非重複性」傳輸之相關章節。[35]資料輸出者需仔細評估每一具體個案。

2.6 Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent – (49 (1) (f))

2.6 第 49 條第 1 項第 f 款 – 於當事人身體上或法律上無法為同意之表示時，傳輸對保護當事人或其他人之重大利益為必要

The derogation of Article 49 (1) (f) obviously applies when data is transferred in the event of a medical emergency and where it is considered that such transfer is directly necessary in order to give the medical care required.

第 49 條第 1 項第 f 款的例外情形明顯適用於發生醫療緊急情況時資料傳輸之情形，尤其是當資料之傳輸係為提供所需的醫療服務為直接必要時。

Thus, for example, it must be legally possible to transfer data (including certain personal data) if the data subject, whilst outside the EU, is unconscious and in need of urgent medical care, and only an exporter (e.g. his usual doctor), established in an EU Member State, is able to supply these data. In such cases the law assumes that the imminent risk of serious harm to the data subject outweighs data protection concerns.

因此，例如，若當事人位於歐盟境外，在無意識並需要緊急醫療護理的情況下，

[35] Page 4.
第 4 頁(譯註：即本翻譯文件第 8 頁)。

且只有位於歐盟成員國境內的資料輸出者（例如他的常用醫生）能夠提供這些資料，則必須得以合法傳輸資料（包括某些個人資料）。在此情形下，法律假定對當事人造成嚴重損害的緊急風險勝過對資料保護之疑慮。

The transfer must relate to the individual interest of the data subject or to that of another person's and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this derogation cannot be used to justify transferring personal medical data outside the EU if the purpose of the transfer is not to treat the particular case of the data subject or that of another person's but, for example, to carry out general medical research that will not yield results until sometime in the future.
傳輸必須涉及當事人或其他人之個人利益，且當傳輸與健康資料有關時，該資料須以進行必要之診斷為必要。因此，若傳輸之目的不是為了在特定情況下治療當事人或另一人之健康情形，而是為例如進行一般醫學研究，且其成果僅會發生於未來某個時點，則例外情形不得作為此類傳輸個人醫療資料至歐盟境外的合理依據。

Indeed, the GDPR does not restrict the use of this derogation to the physical integrity of a person but also leaves room for example to consider the cases where the mental integrity of a person should be protected. In this case, the person concerned would also be incapable - physically or legally - of providing his/her consent for the transfer of his/her personal data. In addition, the concerned individual whose personal data are the subject of the transfer specifically must not be able to give his/her consent – physically or legally - to this transfer.
實際上，GDPR 並沒有將此類例外情形的適用限縮在個人身體完整性，而是保留空間以考量個人精神完整性應受保護之情況。於此情形下，系爭之個人 – 不論在身體或法律上 – 可能無能力對傳輸其個人資料之行為給予同意。此外，當系爭個人之個人資料是傳輸的主要目標時，當事人必須在 – 身體或法律上 – 無能力同意該傳輸。

However, whenever the data subject has the ability to make a valid decision, and his/her consent can be solicited, then this derogation cannot apply.
然而，只要當事人有能力做出有效決定，並且可以徵求其同意，此類例外情形即不適用。

For example, where the personal data is required to prevent eviction from a property, this would not fall under this derogation as, even though housing be considered as a vital interest, the person concerned can provide his/her consent for the transfer of his/her data.
例如，所需之個人資料係為防止從房產中被驅逐，此時不適用例外情形，因為即使居所被認為是一種至關重大的利益，當事人仍可提供對其資料傳輸之同意。

This ability to make a valid decision can depend on physical, mental but also legal incapability. A legal incapability can encompass, without prejudice to national representation mechanisms, for example, the case of a minor. This legal incapability has to be proved, depending on the case, through either a medical certificate showing the mental incapability of the person concerned or through a governmental document confirming the legal situation of the person concerned.
能否做出有效決定可取決於身體和精神狀態，但也包含是否具備法律上的行為能力。例如，在不牴觸國家代理體系的情況下，法律上的無能力可包括因未成年而無行為能力之情形。證明這種法律上的無行為能力，必須依據具體情況，透過得顯示當事人精神上無能力的醫療證明或透過政府文件確認該當事人為法律上無行為能力者。

Data transfers to an international humanitarian organization, necessary to fulfil a task under the Geneva Conventions or to comply with international humanitarian law applicable in armed conflict may also fall under Article 49 (1) (f), see recital 112. Again, in such cases the data subject needs to be physically or legally incapable of giving consent.
為履行「日內瓦公約」中之任務或遵守於武裝衝突時所適用之國際人道法所必需時，得依第 49 條第 1 項第 f 款向國際人道主義組織傳輸資料，請參見前言第 112 點。同樣，在此情形下，當事人必需在身體或法律上無能力給予同意。

The transfer of personal data after the occurrence of natural disasters and in the context of sharing of personal information with entities and persons for the purpose of rescue and retrieval operations (for example, relatives of disaster victims as well as with government and emergency services), can be justified under this derogation. Such unexpected events (floods, earthquakes, hurricanes etc.) can warrant the urgent transfer of certain personal data to learn for example, the location and status of victims. In such situations it is considered that the data subject concerned is unable to provide his/her

consent for the transfer of his/her data.
自然災害發生後個人資料之傳輸，以及為了救援和恢復行動而與法律實體和他人（例如，災民親屬以及政府和緊急服務組織）分享個人資料之情事，可適用此類例外情形。意外災害（洪水、地震、颶風等）之發生可作為緊急傳輸某些個人資料之合理依據，例如為了掌握受災者的位置和狀態。在此情形下，當事人被視為無能力對傳輸其個人資料之行為給予同意。

2.7. Transfer made from a public register - (49 (1) (g) and 49 (2))
2.7. 第 49 條第 1 項第 g 款及第 49 條第 2 項 – 由公眾登記處所為之傳輸

Article 49 (1) (g) and Article 49 (2) allow the transfer of personal data from registers under certain conditions. A register in general is defined as a "*(written) record containing regular entries of items or details" or as "an official list or record of names or items* » [36], where in the context of Article 49, a register could be in written or electronic form.
第 49 條第 1 項第 g 款和第 49 條第 2 項允許在某些條件下傳輸公眾登記之個人資料。登記一般被定義為「*（書面）記錄，包含常規項目或細節的記載*」或「*姓名或項目的正式清單或記錄*」[36]，在第 49 條的範圍內，登記得以書面或電子形式呈現。

The register in question must, according to Union or Member State law, be intended to provide information to the public. Therefore, private registers (those in the responsibility of private bodies) are outside of the scope of this derogation (for example private registers through which credit-worthiness is appraised.
依據歐盟或成員國之法律，登記旨在向公眾提供資訊。因此，私人登記（由私人機構負責）則不屬於此類例外情形之範圍（例如，為評估信用價值所為之私人登記）。

The register must be open to consultation by either:
登記必須對下列任一請求者開放查詢/諮詢：

(a) the public in general or
一般民眾，或

[36] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.01.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.01.2018).
美國韋氏字典，https://www.merriam-webster.com/dictionary/register (22.01.2018)；牛津字典 https://en.oxforddictionaries.com/definition/register (22.01.2018)。

(b) any person who can demonstrate a legitimate interest.

任何得舉證具正當利益者。

These could be, for example: registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers.

這些可以是，例如：公司登記、協會登記、刑事犯罪登記、（土地）所有權登記或公眾車輛登記。

In addition to the general requirements regarding the set-up of the registers themselves, transfers from these registers may only take place if and to the extent that, in each specific case, the conditions for consultation that are set forth by Union or Member State law are fulfilled (regarding these general conditions, see Article 49 (1) (g).

除了關於設置登記本身的一般要求外，在每種特定情況下，只有當歐盟或成員國法律所規定之查詢/諮詢要件被滿足時，始得自登記者進行傳輸。（相關一般要件，請參閱第 49 條第 1 項第 g 款）。

Data controllers and data processors wishing to transfer personal data under this derogation need to be aware that a transfer cannot include the entirety of the personal data or entire categories of the personal data contained in the register (Article 49 (2)). Where a transfer is made from a register established by law and where it is to be consulted by persons having a legitimate interest, the transfer can only be made at the request of those persons or if they are recipients, taking into account of the data subjects' interests and fundamental rights[37]. On a case by case basis, data exporters, in assessing whether the transfer is appropriate, would always have to consider the interests and rights of the data subject.

希望依據此例外情形傳輸個人資料的資料控管者和資料受託運用者需要瞭解不得傳輸登記內全部個人資料或個人資料之所有類別（第 49 條第 2 項）。若傳輸資料係來自法定登記者且要求查詢/諮詢之個人具正當利益，傳輸僅得在其請求下，或若其為接收者時始得發生，且應考量當事人之利益和基本權利。[37]依據個案情形，資料輸出者在評估傳輸是否合適時，必須始終考量當事人的利益和權利。

[37] Recital 111 of the GDPR.
請參閱 GDPR 前言第 111 點。

Further use of personal data from such registers as stated above may only take place in compliance with applicable data protection law.
進一步使用上述登記中之個人資料必須遵守所適用之個人資料保護法。

This derogation can also apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).
這類例外情形亦適用於公務機關執行公權力之活動（第 49 條第 3 項）。

2.8. Compelling legitimate interests – (49 (1) § 2)
2.8. 第 49 條第 1 項第 2 段 – 必要正當利益

Article 49 (1) § 2 introduces a new derogation which was not previously included in the Directive. Under a number of specific, expressly enumerated conditions, personal data can be transferred if it is necessary for the purposes of compelling legitimate interests pursued by the data exporter.
第 49 條 1 項第 2 段加入了先前指令中並未規範之新的例外情形。若符合各項具體、明確列舉之要件，且為資料輸出者追求必要正當利益所必須，得進行個人資料之傳輸。

This derogation is envisaged by the law as a last resort, as it will only apply where "*a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable*".[38]
法律將此類型之例外情形作為最後手段，因其僅適用於當「*傳輸無法符合第 45 條或第 46 條之規定，包括有拘束力之企業守則之規定，且無法適用任何特定例外之情形*」。[38]

This layered approach to considering the use of derogations as a basis for transfers requires consideration of whether it is possible to use a transfer tool provided in Article 45 or 46 or one of the specific derogations set out in Article 49 (1) § 1, before resorting to the derogation of Article 49 (1) §2. This can only be used in residual cases according to recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR[39] the data exporter must be therefore able to demonstrate that it was neither possible to

[38] Article 49 (1) § 2 GDPR.
請參閱第 49 條第 1 項第 2 段。

frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1.
以此種階層式分析法作為考量使用例外情形之基礎，在訴諸第 49 條第 1 項第 2 段例外情形前，須考慮是否得使用第 45 條或第 46 條所規定之傳輸方法或第 49 第 1 項第 1 段規定之特定例外情形之一。依據前言第 113 點，第 2 段所規定之例外情形僅得適用於剩餘案件，且須取決於法律明文規定之諸多條件。因此，依據 GDPR[39]所規範之課責原則，資料輸出者必須能夠證明其無法依第 46 條，對資料之傳輸提供適當安全維護措施，亦無法適用第 49 條第 1 項第 1 段所列舉之任何例外情形。

This implies that the data exporter can demonstrate serious attempts in this regard, taking into account the circumstances of the data transfer. This may for example and depending on the case, include demonstrating verification of whether the data transfer can be performed on the basis of the data subjects' explicit consent to the transfer under Article 49 (1) (a). However, in some circumstances the use of other tools might not be practically possible. For example, some types of appropriate safeguards pursuant to Article 46 may not be a realistic option for a data exporter that is a small or medium-sized company.[40] This may also be the case for example, where the data importer has expressly refused to enter into a data transfer contract on the basis of standard data protection clauses (Article 46 (2) (c)) and no other option is available (including, depending on the case, the choice of a different "data importer") – see also the paragraph below on 'compelling' legitimate interest.
此意味著，資料輸出者可證明其在考量資料傳輸情況時，在這方面所做的各種認真嘗試。這必須取決於具體情況，例如包括證明資料傳輸是否得依第 49 條第 1 項第 a 款之規定，基於當事人明確同意而為之。然而，在某些情況下，援引其他方法有實際執行之困難。例如，對於中小型的資料輸出者而言，第 46 條規範之某些類型的適當安全維護措施可能不是一個實際可行的選擇。[40]又例如，資料輸入者明確拒絕簽訂依據標準資料保護條款（第 46 條第 2 項 c 款）而訂定之資料傳輸契約，且無其他選擇（依據具體情況而定，包括不同「資料輸入者」之選擇）的情形 – 另請參閱下文關於「必要」正當利益之說明。

[39] Article 5 (2) and Article 24 (1)
請參閱第 5 條第 2 款和第 24 條第 1 款。
[40] For example binding corporate rules may often not be a feasible option for small and medium-sized enterprises due to the considerable administrative investments they imply.
例如，因其意味著大量行政投資，具有約束力之企業守則可能經常不適用於中小型企業。

Compelling legitimate interests of the controller

控管者之必要正當利益

According to the wording of the derogation, the transfer must be necessary for the purposes of pursuing compelling legitimate interests of the data controller which are not overridden by the interests or rights and freedoms of the data subject. Consideration of the interests of a data exporter in its capacity as data processor or of the data importer are not relevant.

依據例外情形之用詞，傳輸係資料控管者為追求其必要正當利益所必須，且該利益不得凌駕於當事人之利益或權利及自由。以資料受託運用者之身分考量資料輸出者之利益或考量資料輸入者之利益皆與此規定無關。

Moreover, only interests that can be recognized as "compelling" are relevant and this considerably limits the scope of the application of the derogation as not all conceivable "legitimate interests" under Article 6 (1) (f) will apply here. Rather a certain higher threshold will apply, requiring the compelling legitimate interest to be essential for the data controller. For example, this might be the case if a data controller is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business.

此外，僅有當利益係「必要」時始具有相關性。此一要件大量限縮例外情形的適用範圍，因並非所有第 6 條第 1 項第 f 款可預見之「正當利益」皆適用於此處。相反的，本條適用更高之門檻，要求必要正當利益對資料控管者為必須。例如，若資料控管者必須傳輸個人資料以保護其組織或系統免受嚴重的立即傷害或足以嚴重影響其業務的嚴厲懲罰，也許適用此一情形。

Not repetitive

非重複性

According to its express wording, Article 49 (1) § 2 can only apply to a transfer that is not repetitive[41].

依據其明確之用詞，第 49 條第 1 項第 2 段僅適用於不重複之傳輸。[41]

Limited number of data subjects

有限數量之當事人

[41] For more information on the term « not repetitive » see page 4.
有關「非重複性」一詞更多的解釋，請參閱第 4 頁(譯註：即本翻譯文件第 8 頁)。

Additionally, the transfer must only concern a limited number of data subjects. No absolute threshold has been set as this will depend on the context but the number must be appropriately small taking into consideration the type of transfer in question.
此外，傳輸僅得涉及有限數量的當事人。此處並未設置絕對的門檻，因這將取決於具體情形，但考慮到此傳輸類型具爭議，受影響之當事人數量必須為適當的少數。

In a practical context, the notion "limited number of data subjects" is dependent on the actual case in hand. For example, if a data controller needs to transfer personal data to detect a unique and serious security incident in order to protect its organization, the question here would be how many employees' data the data controller would have to transfer in order to achieve this compelling legitimate interest.
在實際情況中，「有限數量之當事人」的概念取決於具體個案。例如，若資料控管者為保護其組織，需要傳輸個人資料以檢測特殊且嚴重的安全事件，此處之問題在於資料控管者必須傳輸多少員工資料才能實現其必要之正當利益。

As such, in order for the derogation to apply, this transfer should not apply to all the employees of the data controller but rather to a certain confined few.
因此，為了適用例外情形，該傳輸不得適用於資料控管者的所有員工，而應受限適用於某些少數員工。

Balancing the "compelling legitimate interests of the controller" against the "interests or rights and freedoms of the data subject" on the basis of an assessment of all circumstances surrounding the data transfer and providing for suitable safeguards
在評估資料傳輸的所有情狀並提供適當安全維護措施的基礎上，就「控管者的必要正當利益」與「當事人的利益或權利及自由」做平衡

As a further requirement, a balancing test between the data exporter's (compelling) legitimate interest pursued and the interests or rights and freedoms of the data subject has to be performed. In this regard, the law expressly requires the data exporter to assess all circumstances of the data transfer in question and, based on this assessment, to provide "suitable safeguards" regarding the protection of the data transferred. This requirement highlights the special role that safeguards may play in reducing the undue impact of the data transfer on the data subjects and thereby in possibly influencing the balance of rights and interests to the extent that the data controller's interests will not

be overridden.[42]

基於進一步的要求，必須在資料輸出者所追求之（必要的）正當利益與當事人的利益或權利及自由之間進行平衡判斷。在此方面，法律明確要求資料輸出者評估有關資料傳輸的所有情狀，並依據該評估，提供關於保護所傳輸資料之「適當安全維護措施」。此一要求強調了安全維護措施就減少資料傳輸對當事人的不當衝擊可能扮演之特殊角色，從而可能影響權利和利益的平衡，使資料控管者之利益不致被否決。[42]

As to the interests, rights and freedoms of the data subject which need to be taken into consideration, the possible negative effects, i.e. the risks of the data transfer on any type of (legitimate) interest of the data subject have to be carefully forecasted and assessed, by taking into consideration their likelihood and severity.[43] In this regard, in particular any possible damage (physical and material, but also non-material as e.g. relating to a loss of reputation) needs to be taken into consideration[44]. When assessing these risks and what could under the given circumstances possibly be considered as "suitable safeguards" for the rights and freedoms of the data subject, the data exporter needs to particularly take into account the nature of the data, the purpose and duration of the processing as well as the situation in the country of origin, the third country and, if any, the country of final destination of the transfer.[45]

至於需要被考量之當事人的利益、權利及自由，必須仔細預測和評估可能的負面影響，即資料傳輸對當事人任何類型的（正當）利益所受之諸多可能且嚴重之風險。[43]在此情形下，特別是任何可能之損害（人身和財物，但也包括例如與喪失聲譽有關之非財物損害）皆須列入考量。[44]在評估此些風險以及在特定情況下可能被視為係提供當事人權利和自由的「適當保障」措施，資料輸出者需特別考量

[42] The important role of safeguards in the context of balancing the interests of the data controller and the data subjects has already been highlighted by the Article 29 Working Party in WP 217, p. 31.
第 29 條工作小組在 WP217 中已強調安全維護措施在平衡資料控管者和當事人利益方面所扮演之重要角色（第 31 頁）。

[43] See Recital 75: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity (...)".
請參閱前言第 75 點：「自然人的權利及自由產生不同可能性與嚴重性的風險（.....）」。

[44] See Recital 75: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage."
請參閱前言第 75 點：「個人資料運用可能導致自然人的權利及自由產生不同可能性與嚴重性的風險，恐造成人身、財物或非財物的損害」。

資料的性質、資料運用目的和持續時間以及傳輸原始國、第三國和最終目的地國家（如果有的話）的情況。[45]

Furthermore, the law requires the data exporter to apply additional measures as safeguards in order to minimize the identified risks caused by the data transfer for the data subject.[46] This is set up by the law as a mandatory requirement, so it can be followed that in the absence of additional safeguards, the controller's interests in the transfer will in any case be overridden by the interests or rights and freedoms of the data subject.[47] As to the nature of such safeguards, it is not possible to set up general requirements applicable to all cases in this regard, but these will rather very much depend on the specific data transfer in question. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data.[48] Moreover, technical and organizational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter should be examined.
此外，法律要求資料輸出者採取額外措施作為保障，以盡量減少傳輸對當事人帶來的已識別風險。[46]這是法律所規定之強制性要求，因此可認為在沒有額外安全維護措施的情形下，當事人之利益或權利及自由得在任何情況優於控管者在傳輸中之利益。[47]有鑒於此種安全維護措施之性質，該措施之要件在很大程度上需取決於系爭特定資料傳輸，而無法制定適用於所有情況之一般要件。依據個案，安

[45] Recital 113.
請參閱前言第 113 點。
[46] While in the context of an "ordinary" balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Working document on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214), p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the "balancing test" and therefore to be feasible under this derogation.
雖然在法律可預見之「一般」平衡判斷的背景下，並非在每種情形皆需要此些（額外的）措施（請參閱第 29 條工作小組關於「歐盟資料受託運用者對非歐盟轉承包受託運用者」之特定目的契約條款草案工作文件（WP 214），第 41 頁），第 49 條第 1 項第 2 段之用詞闡明，為適用此例外情形，必須採行其他措施，使資料移轉符合「平衡判斷」。
[47] While in the context of an "ordinary" balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the "balancing test" and therefore to be feasible under this derogation.
雖然在法律可預見之「一般」平衡判斷的背景下，並非在每種情形皆需要此些（額外的）措施（請參閱第 29 條工作小組意見 06/2014，依據第 95/46/EC 號指令第 7 條規定關於資料控管者之正當利益概念，WP217，第 41 頁），第 49 條第 1 項第 2 段之用詞闡明，為適用此例外情形，必須採行其他措施，使資料移轉符合「平衡判斷」。

全維護措施可能包括確保在傳輸後將儘快刪除資料或限制傳輸後資料運用目的之措施。應特別注意傳輸假名化或加密資料是否足夠。[48]此外，應審查旨在確保傳輸之資料不得用於資料輸出者嚴格可預見目的以外之技術性及組織性措施。

Information of the supervisory authority
監管機關之資訊

The duty to inform the supervisory authority does not mean that the transfer needs to be authorized by the supervisory authority, but rather it serves as an additional safeguard by enabling the supervisory authority to assess the data transfer (if it considers it appropriate) as to its possible impact on the rights and freedoms of the data subjects affected. As part of its compliance with the accountability principle, it is recommended that the data exporter records all relevant aspects of the data transfer e.g. the compelling legitimate interest pursued, the "competing" interests of the individual, the nature of the data transferred and the purpose of the transfer.
告知監管機關之義務並非意味著傳輸需得到監管機關之授權，而是一種額外的安全維護措施，藉由監管機關來評估該資料傳輸（若其認為適當之情形）對受影響之當事人的權利和自由可能產生之衝擊。作為遵守課責性原則的一部分，建議資料輸出者記錄和資料傳輸所有相關資訊，例如：所追求之必要正當利益、個人的「競爭」利益、傳輸資料之性質以及傳輸之目的。

Providing information of the transfer and the compelling legitimate interests pursued to the data subject
提供當事人有關傳輸之資訊及所追求之必要正當利益

The data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued. This information must be provided in addition to that required to be provided under to Articles 13 and 14 of the GDPR.
資料控管者必須將傳輸及所追求之必要正當利益告知當事人。除了依據 GDPR 第 13 條和第 14 條要求提供之資訊外，尚需提供此資訊。

[48]For other examples of possible safeguards see Article 29 Working Party Working document on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214), p. 41-43
關於安全維護措施的其他可能範例，請參閱第 29 條工作小組關於「歐盟資料受託運用者對非歐盟轉承包受託運用者」之特定目的契約條款草案工作文件（WP 214），第 41-43 頁。

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

關於第2016/679號規則(GDPR)中的個人資料侵害通知之指引

Adopted on 3 October 2017

2017年10月3日通過

As last Revised and Adopted on 6 February 2018

2018年2月6日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013號辦公室。

Website：http：//ec.europa.eu/justice/data-protection/index_en.htm
網址：http：//ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日之第95/46/EC號指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES：

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

TABLE OF CONTENTS 目錄

INTRODUCTION 導言

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.
一般資料保護規則（GDPR）要求將個人資料之侵害（此後簡稱為「侵害」）通知國家監管機關[1]（或在跨境侵害之情況下，通知主責機關），並在某些情況下，須向個人資料因侵害而受影響之當事人就侵害進行溝通。

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

---

[1] See Article 4(21) of the GDPR
請參閱 GDPR 第 4 條第 21 款。

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 和 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611。

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
請參閱 https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm。

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046。

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
此為歐盟基本權利憲章所載之權利，請參閱http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT。

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

某些組織目前已存在侵害通知義務，例如公眾電子通信服務提供者（如2009/136/EC指令和第611/2013號規則（EU）中所規定）[2]。也有部分歐盟成員國已有其國內的侵害通知義務，這可能包括某些類別之控管者和公眾電子通信服務提供者的侵害通知義務（例如德國和義大利），或有義務通報所有個人資料侵害案件（例如荷蘭）。其他成員國可能有相關之業務守則（例如愛爾蘭[3]）。雖然許多歐盟資料保護機關目前皆鼓勵控管者通報侵害行為，但被GDPR取代的95/46/EC個人資料保護指令[4]並未包含具體的侵害通知義務，因此對許多組織而言，這將會是一項新的要求。GDPR現在強制要求所有控管者應負通知義務，除非該侵害不太可能對個人的權利和自由造成風險[5]。受託運用者也扮演重要的角色，任何侵害發生必須通知控管者[6]。

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

29條工作小組（WP29）認為此項新的通知要求有許多益處。在通知監管機關時，控管者可就是否需通知受影響之個人獲得建議。當然監管機關可能要求控管者將侵害事件通知該個人[7]。透過與個人溝通侵害事件，控管者可以提供因該侵害所帶來的風險之資訊，以及個人為保護自身免受潛在後果影響得採取之保護措施。任何侵害應變計劃之重點應該著重於保護當事人及其個人資料。因此，侵害通知應被視為係強化關於遵循個人資料保護之工具。同時應注意，漏未向個人或監管機關通知侵害之發生可能意味著第83條之罰鍰可能適用於控管者。

Controllers and processors are therefore encouraged to plan in advance and put in place processes

---

請參閱第 33 條第 2 項。此與（EU）第 611/2013 號規則第 5 條的概念類似，該條款規定，若發生個人資料侵害事件，以契約約定提供部分電子通信服務的提供者（與用戶沒有直接的契約關係）有義務通知契約提供者該侵害。

[7] See Articles 34(4) and 58(2)(e)

請參閱第 34 條第 4 項和第 58 條第 2 項第 e 款。

to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.
因此鼓勵控管者和受託運用者提前計劃並實施相關步驟，以便能夠檢測並迅速控制侵害，進而評估對個人造成之風險[8]，然後確認是否有必要通知監管機關，並在必要時就侵害與相關個人進行溝通。通知監管機關應屬於事故應變計畫之一部分。

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.
GDPR規定了何時需要通知侵害、通知之對象以及通知應包含何種資訊。該通知應包含之資訊可分階段提供，但在任何情形下，控管者皆應及時對任何侵害採取行動。

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.
在關於個人資料侵害通知之03/2014意見中[9]，WP29提供指導以協助控管者判斷在發生侵害時是否應通知當事人。該意見考量了2002/58/EC指令有關電子通信服務提供者之義務，並提供了多個產業的示例，然後以此脈絡草擬GDPR，並為所有控管者提供優良實務範例。

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.
本指引說明了GDPR的強制侵害通知義務和溝通要求，以及控管者和受託運用者為符合其新義務可採取的一些步驟。本文件亦舉例說明了各種類型之侵害以及在不同可能情境下需要

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).
這可以在 DPIA 的監測和審查要求下得到確保，DPIA(個資保護影響評估)對於可能導致自然人權利和自由的高風險的處理操作是必要的（第 35 條第 1 項和第 11 項）。
[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
請參閱關於個人資料侵害通知之 03/2014 意見 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf。

被通知之對象。

I. Personal data breach notification under the GDPR
GDPR之個人資料侵害通知

A. Basic security considerations
基本安全考量因素

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].
GDPR的要求之一，係透過採用適當技術性與組織性措施，個人資料應可以確保適當安全性之方法運用，包括防止未經授權或非法運用以及防止意外遺失、破壞或毀損[10]。

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].
因此，GDPR要求控管者和受託運用者皆須採取適當之技術性與組織性措施，以確保安全層級與運用個人資料產生之風險相當。相關措施應考量到現有技術水準、執行成本和資料運用之性質、範圍、背景及運用目的，以及對自然人權利和自由之風險變動的可能性和嚴重性[11]。此外，不論是否已有侵害發生，GDPR亦要求立即建置所有的適當技術性保護組織措施，以確認該措施是否已包含通知義務[12]。

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.
因此，任何資料安全政策的關鍵要素是，能夠在可能的情況下，防止侵害之發生，並於仍

[10] See Articles 5(1)(f) and 32.
請參閱第 5 條第 1 項第 f 款以及第 32 條。
[11] Article 32; see also Recital 83
第 32 條；另請參閱前言第 83 點。
[12] See Recital 87
請參閱前言第 87 點。

發生侵害情事時，及時對其作出反應。

B. What is a personal data breach？

何謂個人資料侵害?

1. Definition

定義

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a “personal data breach” in Article 4(12) as：

因應侵害的第一步是控管者須先能識別該侵害。GDPR第4條第12款將「個人資料侵害」定義為：

> “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
>
> 「違反安全性導致傳輸、儲存或以其他方式運用之個人資料遭意外或非法破壞、遺失、變更、未經授權揭露或存取使用。」

What is meant by “destruction” of personal data should be quite clear： this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. “Damage” should also be relatively clear： this is where personal data has been altered, corrupted, or is no longer complete. In terms of “loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

「破壞」個人資料之定義應已非常明確：係指資料不存在，或不再以對控管者有用之形式存在。「毀損」之定義也應相對明確：係指個人資料已被更改、損毀或不再完整。就個人資料「遺失」而言，應可被解釋為資料可能仍然存在，但控管者失去對該資料之控制或存取，或不再擁有該資料。最後，未經授權或非法運用可能包括向未被授權接收（或存取）資料之接收者揭露（或使其存取）個人資料，或違反GDPR規範之其他任何形式之運用。

Example
示例

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.
個人資料遺失之示例可包括控管者客戶資料庫副本儲存設備遺失或遭竊。遺失的另一個例子可能是個人資料集的唯一副本已被勒索軟體加密，或者已被控管者加密卻不再擁有加密金鑰。

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].
侵害屬於一種安全事故應已十分明確。然而，如第4條第12款所示，GDPR僅適用於侵害*個人資料*之情事。侵害發生之後果在於控管者將無法確保遵守GDPR第5條所規範之個人資料運用相關原則。這突顯了安全事故和個人資料侵害之間的區別 – 本質上，雖然所有個人資料侵害皆屬於安全事故，但並非所有的安全事故都必然是個人資料之侵害[13]。

The potential adverse effects of a breach on individuals are considered below.
侵害對個人的潛在不利影響說明如下。

2. Types of personal data breaches
個人資料侵害類型

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]：

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.
應該注意的是，安全事件不僅限於從外部來源對組織進行攻擊之威脅型態，而亦包括因內部運用違反安全原則之事件。
[14] See Opinion 03/2014
請參閱 03/2014 意見。

WP29在03/2014關於侵害通知之意見中說明，「侵害」可依據以下三項著名的資訊安全原則進行分類[14]：

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
  「機密性之侵害」- 未經授權或意外揭露或存取個人資料之情形。

- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
  「完整性之侵害」- 未經授權或意外變更個人資料之情形。

- "Availability breach" - where there is an accidental or unauthorised loss of access[15]to, or destruction of, personal data.
  「可用性之侵害」- 意外或未經授權遺失存取[15]或破壞個人資料之情形。

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.
亦需注意，依情況，侵害可能同時涉及個人資料之機密性、完整性和可用性，及其任何組合。

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.
是否存在機密性或完整性侵害相對而言較為明確，而是否存在可用性侵害則較不明顯。當個人資料永久遺失或破壞時，皆會被認為是可用性侵害。

---

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information," available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: " Timely, reliable access to data and information services for authorized users." See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en
一般公認「存取」基本上屬於「可用性」之一環。 例如，請參閱NIST SP800- 53rev4將「可用性」定義為：「確保得及時且確實存取和使用資訊」。請查詢 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf。CNSSI-4009亦提及：「為授權用戶提供及時且確實存取資料和資訊服務。」請參閱https://rmf.org/wp- content/uploads/2017/10/CNSSI-4009.pdf. 。ISO/IEC 27000：2016亦將「可用性」定義為「依據授權實體之要求可存取和使用之資產」：https://www.iso.org/obp/ui/#iso:std:iso- iec:27000:ed-4:v1:en。

Example
示例

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.
遺失可用性之示例包括資料被意外或未經授權之人刪除，或遺失安全加密資料的解密金鑰。若控管者無法恢復對資料之存取，例如，從備份中恢復，則這將被視為永久遺失可用性。

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.
若組織的正常服務受到嚴重干擾，也可能會造成可用性遺失，例如，遇到電源故障或阻斷服務攻擊，導致無法使用個人資料。

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".
可能會被提出的問題是，暫時喪失個人資料可用性是否應被視為可用性之侵害，若是，則需通知。GDPR第32條「運用之安全」說明，在實施技術性與組織性措施以確保安全層級與風險相當時，除其他要件外，「可持續確保運用系統和服務之機密性、完整性、可用性和彈性的能力」，與「在實體環境或技術性事故中，能及時恢復個人資料的可用性和存取的能力」亦應納入考量。

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12).

因此，導致個人資料在一段時間內無法使用的安全事故也屬於一種侵害，因為無法存取資料會對自然人之權利和自由產生重大影響。明確地說，因執行計畫性之系統維護而無法存取個人資料不屬於第4條第12款所定義之「安全性之侵害」。

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

與個人資料之永久遺失或破壞（或實際上任何其他類型之侵害）相同，涉及暫時喪失可用性之侵害應依據第33條第5項予以記錄。這有助於控管者向監管機關證明其責任，監管機關可能會要求查看該紀錄[16]。然而，依據侵害情況，可能需要通知監管機關及與受影響之個人溝通，也可能不需要。控管者將需評估因缺乏個人資料之可用性，對自然人權利和自由影響的可能性和嚴重性。依據第33條，除非該侵害不太可能對個人之權利和自由造成風險，否則控管者將需要通知。當然，這將需要依據個案進行評估。

[16] See Article 33(5)
請參閱第 33 條第 5 項。

Examples

示例

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.
在醫院中，若無法使用關於病患的關鍵醫療資料，即使是暫時的，亦會對個人之權利和自由帶來風險；例如，手術可能被取消並將患者生命置於危險之中。

Conversely, in the case of a media company's systems being unavailable for several hours (e.g.due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.
反之，在數小時無法使用媒體公司系統的情況下（例如因為停電），若該公司因此無法向其用戶發送定期通訊，則不太可能對個人的權利和自由構成風險。

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.
應注意的是，儘管控管者的系統可能只是暫時喪失可用性，且可能不會對個人產生影響，但重要的是，控管者仍必須考量該侵害所有可能造成的後果，因為控管者可能因其他原因仍負通知義務。

Example

示例

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.
若可從備份中恢復資料，感染勒索軟體（惡意軟體加密控管者之資料直到支付贖金）可能會導致暫時失去資料的可用性。然而，網路入侵已發生，若該事故符合機密性之侵害（例如個人資料遭攻擊者存取之情形），對個人的權利和自由造成風險，則可能需要通知。

3. The possible consequences of a personal data breach
個人資料侵害之可能後果

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[17].
侵害可能會對個人產生一系列潛在的重大不利影響，從而導致人身、財物或非財物的損害。GDPR說明這可能包括失去對個人資料之控制、對其權利之限制、歧視、冒用身分或詐欺、財務損失、未經授權之假名化還原、名譽損害以及受專業秘密保護之個人資料機密性之喪失。此亦包括其他任何對個人經濟的或社會的重大不利益之情形[17]。

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].
因此，GDPR要求控管者將侵害通知權責監管機關，除非不太可能導致此類不利影響之風險發生。若發生此類不利影響之風險甚高，則GDPR要求控管者在合理可行的情況下儘速與受影響之個人就該侵害進行溝通[18]。

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR：
GDPR前言第87點強調能夠識別侵害、評估其對個人之風險以及在必要時通知之重要性：

[17] See also Recitals 85 and 75.
請參閱前言第 85 點及第 75 點。
[18] See also Recital 86.
請參閱前言第 86 點。

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."
「應查明是否已實行所有適當之技術性保護與組織性措施，以便立即確認個人資料侵害是否發生，並快速通知監管機關和當事人。通知並未無故遲延之事實，尤應考量個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響。該通知可能導致監管機關依據本規則所訂定之任務或權力進行干預。」

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.
對個人不利影響之風險評估相關指引請參見第IV節。

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state： "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889
詳細資訊請參閱 29 條工作小組關於適用與訂定行政罰鍰之指引，請查閱：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889。

(Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

若控管者漏未通知監管機關與受侵害之當事人或其中一方，即使已符合第33條和/或第34條之要求，監管機關得依據第58條第2項之規定或其自身之決定，就所有可行之矯正措施做出選擇，包括考量處以適當之行政罰鍰[19]。若其選擇行政罰鍰，依據GDPR第83條第4項第a款，可處以最高10,000,000歐元或企業前一年度全球年營業額2%之罰鍰。亦須注意的是，在某些情況下，漏未進行侵害通知可能顯示現有安全措施之缺乏或現有安全措施之不足。WP29關於行政罰鍰之指引敘明：「在任何特定單一案件中，同時發生若干不同之侵害行為，意味著監管機關能夠在最嚴重侵害之範圍內，對其處以有效、符合比例和具有勸阻性程度之行政罰鍰」。在此情形下，監管機關亦可能一方面就漏未通知或溝通侵害事故（第33條和第34條）處罰，另一方面就缺乏（適當的）安全措施（第32條）予以處罰，因其屬兩種單獨的侵害行為。

II. Article 33 - Notification to the supervisory authority

第33條 - 通知監管機關

A. When to notify

何時通知

1. Article 33 requirements

第33條之要求

Article 33(1) provides that：

第33條第1項規定：

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."
>
> 「於個人資料侵害發生時，控管者即應依第55條通報權責監管機關，不得無故遲延，且如可能，應於知悉後72小時內通報，但個人資料侵害不致對當事人權利和自由造成風險時，不在此限。如未能於72小時內通報監管機關，通報時應併附遲延之理由。」

Recital 87 states[20]：

前言第87點指出[20]：

> "It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."
>
> 「應查明是否已實行所有適當之技術性保護與組織性措施，以立即確認個人資料侵害是否發生，並快速通知監管機關與當事人。判斷該通知非無故遲延之事實，尤應考量對個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響。該通知可能導致監管機關依據本規則所訂定之任務或權力進行干預。」

2. When does a controller become "aware"?

   控管者「知悉」之時點為何？

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

如上所述，GDPR要求，在侵害發生時，控管者應在沒有不當遲延的情況下通知侵害行為，且如可能，應於知悉後72小時內為之。此處的問題是何時得認定控管者已「知悉」侵害之發生。WP29認為，當控管者就發生危及個人資料的安全事故已具有合理程度的確定時，該控管者應可被認定為已「知悉」。

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into

[20] Recital 85 is also important here.
前言第 85 點於此處亦同等重要。

account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

然而，如前所述，GDPR要求控管者實施所有適當之技術性保護與組織性措施，以立即確認是否有侵害發生，並及時通知監管機關和當事人。此外，判斷該通知非無故遲延之事實，尤應考量對個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響[21]。這使控管者有義務確保及時「知悉」任何侵害情事，以便採取適當的行動。

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

要確切認定何時控管者得被視為「知悉」特定之侵害，將取決於具體侵害之情況。在某些情況下，侵害從一開始就相對明顯，而於其他情況，則需要時間判斷是否已危及個人資料。然而，重點應在於迅速採取行動調查事故，以確認個人資料是否確實遭到侵害，如果是，則採取補救措施並在必要時通知。

[21] See Recital 87
請參見前言第 87 點。

Examples

示例

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.
在遺失存有未加密個人資料的USB 智能儲存裝置*的情況下，通常不可能確認未授權之人是否已存取該資料。然而，即使控管者可能無法確認是否發生機密性侵害，但由於發生侵害之可能性已具有合理程度的確定性，因此必須通知。當控管者瞭解到USB智能儲存裝置遺失時，可被視為「知悉」。

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".
第三方通知控管者，他們意外取得其一位客戶的個人資料，並提供該項資料係未經授權揭露之證據。由於控管者已經獲得機密性侵害的明確證據，因此毫無疑問地，控管者可被視為「知悉」。

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".
控管者偵測到其網路可能遭受入侵。經控管者檢查其系統並確認該系統所保存之個人資料已受危害。由於控管者現已有侵害的明確證據，因此毫無疑問地可被視為「知悉」。

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.
一名網路罪犯於駭入控管者之系統後與其聯繫以勒索贖金。於此情形下，在檢查其系統並確認已遭到攻擊後，控管者已有發生侵害的明確證據，因此毫無疑問可被視為「知悉」。

*註釋：USB Key是一種智能儲存裝置，有CPU晶片可進行加解密運算，通常用於身分認證，與一般USB隨身碟不同。

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short

period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

控管者於首次經由個人、媒體組織或其他來源告知可能發生侵害，或自行偵測到安全事故時，可進行短期調查，以確認侵害是否確實發生。在此調查期間，控管者得不被視為已「知悉」。然而，應盡快展開初步調查，並以合理程度的確信來判斷是否發生侵害；之後再進行更詳細之調查。

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

一旦控管者已知悉，屬應通知之侵害應立即通報，不得無故遲延，且如果可能，該通報不得晚於72小時。在此期間，控管者應評估個人可能面臨之風險，以決定是否已觸發通報要求，以及處理侵害所需之行動。然而，控管者或許已對侵害可能導致之潛在風險進行初步評估，該初步評估可能來自於執行相關運用操作前所進行的個資保護影響評估（DPIA）[22]其中一部分。然而，與任何實際侵害的特定情狀相比，DPIA(評估的情況)可能較為一般，因此無論如何，都需在考量上開特定情狀下進行額外之評估。有關風險評估的進一步資訊，請參閱第IV節。

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

在大多數情況下，於初次預警後，隨後應完成這些初步行動 (即當控管者或受託處理者懷疑發生可能涉及個人資料之安全事故時) – 僅在例外情況下始得允許較長的時間。

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
請參閱 29 條工作小組關於 DPIAs 指引，請查閱 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。

Example

示例

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

當事人通知控管者收到冒充控管者的電子郵件，其中包含與該當事人（實際）使用控管者服務相關之個人資料，意味著控管者的安全性已遭受危害。控管者進行短期調查並確認其網路遭入侵以及未經授權存取個人資料之證據。控管者於此時將被視為「知悉」，並且需通報監管機關，除非該侵害不太可能對個人的權利和自由構成風險。控管者將需採取適當的補救措施來解決該侵害。

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

因此，控管者應有內部流程，以便能夠偵測並處理侵害之發生。例如，為發現非常規之資料運用行為,控管者或受託運用者得使用某些技術性措施,例如資料流和(電腦)日誌分析器，從中藉由任何日誌資料之關聯得以辨識出事件和預警[23]。重要的是，當偵測到侵害時，須向上通報至適當的管理階層，以便於處理，並於符合第33條要件時依該條進行通報、必要時

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.
應當注意，促進例如資料的儲存、修改或刪除的可審計性之日誌資料亦可被認為係與開始相應運用操作之人的相關個人資料。

並依據第34條進行通知。此類措施和通報機制可在控管者的事故應變計畫和/或公司治理規劃中詳細描述。這將有助於控管者有效規劃並確認組織內負責管理侵害之人員以及如何或是否酌情升高事故等級。

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).
控管者亦應與其所使用之任何受託運用者採取適當安排，當發生侵害時，受託運用者有義務通知控管者（請參閱下文）。

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.
控管者和受託運用者有責任採取適當之措施來防止、因應與處理侵害，對此，有一些應適用於所有案件的實際步驟

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
  所有與安全事件相關之資訊應直接交付予負責人員，或其任務為處理事故、確認侵害之存在以及評估風險之人員。

- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
  然後應評估因侵害而導致之個人風險（無風險、風險或高風險之可能性），並通知組織的相關部門。

- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
  必要時，應通報監管機關，並與受影響之當事人就侵害進行可能的溝通。

- At the same time, the controller should act to contain and recover the breach.
  同時，控管者應採取行動以控制和挽救該侵害。

- Documentation of the breach should take place as it develops.
  應全程記錄侵害事故之發展。

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some

investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

因此，很清楚的是，控管者有義務對任何初次預警採取行動，並確認侵害是否實際發生。允許在短暫的期間內進行一些調查，並讓控管者蒐集證據和其他相關詳情。然而，一旦控管者對侵害之發生具有合理程度之確定時，如符合第33條第1項之要件，則應通報監管機關，不得無故遲延，且如果可能，不得晚於72小時[24]。若控管者未能及時採取行動並且顯然確實發生了侵害，則控管者可能被視為未依據第33條進行通報。

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data： the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

第32條明確規範控管者和受託運用者應採取適當技術性與組織性措施，以確保個人資料的適當安全等級：得以及時偵測、處理和報告侵害之能力，應被視為這些措施之基本要素。

3. Joint controllers
共同控管者

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

第26條規範共同控管者，並規定共同控管者應確定為履行GDPR其各自應負之責任[25]。這將包括確定哪一方有依第33條和第34條規定遵守相關義務之責。WP29建議共同控管者間之契約安排應包括確認哪一方控管者將主導或負責遵守GDPR侵害通知義務之規定。

---

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN
請參閱第 1182/71 號規則關於確認適用於期間、日期和時間限制之規則，請查閱：http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN。

[25] See also Recital 79.
請參閱前言第 79 點。

4. Processor obligations

受託運用者之義務

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

控管者就個人資料的保護負有全面性之責任，但受託運用者在協助控管者遵守其義務上扮演重要角色；這包括侵害之通知。實際上，第28條第3項明定受託運用者所為之處理應受契約或其他立法之拘束。第28條第3項第f款指出，契約或其他立法應規定受託運用者「考量運用之性質和受託運用者可得之資訊，協助控管者確保遵守第32至第36條所訂之義務」。

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

第33條第2項明確規定，若控管者利用某受託運用者，且該受託運用者知悉其代表控管者運用之個人資料遭到侵害，則應通知控管者，且「不得無故延遲」。應注意，受託運用者在通知控管者之前不需先行評估因侵害而引起風險的可能性，此為控管者在知悉侵害時所必須進行之評估。受託運用者只需確認是否有侵害之發生並通知控管者。控管者係利用受託運用者來實現其特定目的，因此，原則上一旦受託運用者已向其通知該項侵害，控管者應

被視為「知悉」。受託運用者通知控管者之義務使得控管者得解決侵害，並確認是否需要依據第33條第1項通報監管機關和依據第34條第1項通知受影響之當事人。因受託運用者或許無法獲知所有與該事件相關的事實，所以控管者可能也希望調查該侵害，例如，若控管者仍保留了被受託運用者毀損或遺失的個人資料副本或備份。這可能會影響控管者是否因而需要通知。

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.
GDPR就受託運用者必須於何時限內向控管者提出警示並無明確規定，僅規定「不得無故遲延」。因此，WP29建議受託運用者迅速通知控管者，當獲得更多細節時，可分階段提供有關侵害之進一步資訊。這對於幫助控管者滿足在72小時內向監管機關通知之義務相當重要。

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.
如上所述，控管者和受託運用者間之契約除了需包含GDPR中之其他規範外，應闡明如何滿足第33條第2項所述之要求。這可包括要求受託運用者儘早通知，以協助控管者符合在72小時內向監管機關通報之義務。

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.
若受託運用者提供服務的多個控管者皆受同一事故影響，則受託運用者必須對每個控管者通報該事故的詳細資訊。

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.
若控管者已給予受託運用者適當之授權，且該授權係控管者和受託運用者間契約安排的一部分，則受託運用者可代表控管者進行通知。該通知必須符合第33條和第34條之規定。然而，須特別注意通知的法律責任仍由控管者承擔。

B. Providing information to the supervisory authority
向監管機關提供資訊

1. Information to be provided
所須提供之資訊

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should：
當控管者向監管機關通報侵害時，第33條第3項規定，該通報至少應：

> "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
> 「描述個人資料侵害之性質，如有可能，應包括相關當事人之類別和大致數量，以及相關個人資料紀錄之類別和大致數量；
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
> 告知個資保護長之姓名和聯繫方式，或其他可獲取更多資訊之聯絡點；
>
> (c) describe the likely consequences of the personal data breach;
> 描述個人資料侵害之可能結果
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."
> 描述控管者為解決個人資料侵害而採行或預計採行之措施，在適當情況下，包括降低可能不利影響之措施。」

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach： depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.
GDPR就當事人或個人資料紀錄之類別並無定義。然而，WP29建議當事人之類別係指個人

資料受侵害影響之各類人員：依據所使用之描述，這可能包括兒童及其他弱勢群體、殘疾人士、員工或客戶等。同樣地，個人資料紀錄的類別可指控管者所運用的不同類型之紀錄，例如健康資料、教育紀錄、社會照護資訊、財務細節、銀行帳號，護照號碼等。

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.
前言第85點明確指出，通知的目的之一係限縮對個人造成之損害。因此，若當事人之類型或個人資料之類型顯示因侵害而發生特定損害之風險（例如冒用身分、詐欺、財務損失、對職業秘密之威脅），則於通知中表明這些類別是很重要的。透過此方式，可與描述該侵害可能後果之要求產生連結。

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.
無法掌握準確之資訊（例如受影響當事人的確切數量）不應成為及時通報該侵害之阻礙。GDPR允許就受影響的個人數量和相關個人資料紀錄的數量粗略估計。重點應直接針對解決侵害的不利影響，而非提供準確的數字。

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.
因此，若侵害之發生已十分明確，但侵害程度未明，則分階段通知（見下文）是履行通知義務的安全方式。

Article 33(3) states that the controller “shall at least” provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.
第33條第3項規定，控管者「應至少」於通知中提供該等資訊，使控管者得於必要時選擇提供進一步的細節。不同類型之侵害（機密性、完整性或可用性）可能需要進一步的資訊以充分說明每個案件之情況。

Example

示例

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

若侵害發生之根本原因來自於受託運用者，特別是該事故係因同一受託運用者致使其他許多控管者的個人資料紀錄皆受到影響時，控管者於通報監管機關時，同時告知該受託運用者之名稱將對控管者有所助益。

In any event, the supervisory authority may request further details as part of its investigation into a breach.

無論如何，監管機關可能會要求進一步之細節作為其侵害調查的一部分。

2. Notification in phases

分階段通知

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states：

依據侵害之性質，控管者可能必須做進一步調查，以確認與事故相關之所有事實。因此，第33條第4項規定：

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

「在無法同時提供資訊的情形下，可分階段提供資訊，不得有進一步之無故遲延。」

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29

recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.
此意味著GDPR認識到控管者在知悉侵害後的72小時內並不一定可掌握有關侵害的所有必要資訊，因為在此初始階段可能無法取得完整而全面的事故詳情。因此，GDPR允許分階段通知。此情形在複雜的侵害事故中更有可能發生，例如發生某些類型的網路安全事故時，需要進行深入的司法鑑定調查，以充分確認侵害之性質以及個人資料遭損害之程度。於是在許多情況下，控管者必須進行更多調查，並繼續跟進以取得進一步資訊。因此第33條第1項允許控管者於延遲通報之情況下併附理由。WP29建議，若控管者於首次通報監管機關時尚未取得所有必要資訊，控管者應同時告知監管機關，將於日後提供更多詳細資訊。監管機關應決定該項詳細資訊應如何及何時提供。但若控管者一旦知悉必須提供給監管機關之與侵害相關的其他細節，該決定並不妨礙控管者在任何其他階段提供進一步的資訊。

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.
要求通報之目的係鼓勵控管者對侵害迅速採取行動、控制侵害並儘可能回復受損之個人資料，並向監管機關尋求相關建議。在最初的72小時內通報監管機關可協助控管者確認關於通知或不通知當事人之決定是否正確。

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to

[26] See Article 9.
請參閱第 9 條。

communicate the breach to the data subject where it is required.
然而，通報監管機關之目的不僅在於取得是否應通知受影響當事人之指導。在某些情況下，由於侵害之性質和風險的嚴重程度，控管者很明顯地必須立即通知受影響之當事人，不得遲延。例如，有冒用身分的立即威脅或特殊類別個人資料在線上被揭露[26]時，控管者應採取行動控制侵害並與受影響之當事人就該侵害進行溝通，不得無故遲延(請參閱第III節)。在特殊情況下，甚至可能在通報監管機關前即須採取行動。一般來說，對監管機關之通知不得作為未在需要時與當事人溝通該項侵害之正當理由。

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.
亦應釐清的是，在進行首次通報後，若後續調查證據顯示安全事故已被控制且並無實際侵害發生，控管者可向監管機關更新資訊。這些資訊可增列至已提供給監管機關的資訊中，因此該項紀錄即不屬於侵害事故。通報最後並未造成侵害之事故不會導致罰鍰。

Example
示例

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.
控管者在發現遺失包含某些客戶個人資料副本的USB智能儲存裝置的72小時內通報監管機關。而後發現係控管者內部歸檔錯誤，該USB智能儲存裝置失而復得。控管者向監管機關更新資訊並請求修正通報。

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.
另應注意的是，2002/58/EC指令、第611/2013號規則和其他自行通報事故之現有義務，皆已採用分階段通報方式。

3. Delayed notifications

遲延通報

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

第33條第1項明確規定，若未於72小時內向監管機關通報，則通報應附遲延之理由。依據該規定與分階段通知之概念可知，已認知控管者可能無法皆於規定時間內通報侵害，因此遲延通報可被允許。

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

此種情況可能發生於，例如控管者在短時間內經歷多個相類似的機密性侵害，並同樣影響大量當事人。控管者可能已知悉侵害，同時開始調查，但在通報前，再偵測出不同起因的類似侵害。依據具體情況，控管者可能需要一段時間來確認侵害程度，與其單獨通報各項侵害，不如讓控管者將數個非常相似但起因各異之侵害整理為一份有意義的通報。這就可能導致該項對監管機關之通報遲延並超過控管者首次知悉侵害之72小時。

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a “bundled” notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

嚴格來說，個別侵害皆是可通報事故。然而，為了避免過度負擔，若涉及在相對短時間內以相同之方式侵害相同類型之個人資料，控管者可提交包含所有侵害之「包裹」通報。若涉及不同類型個人資料的一連串侵害，且以不同方式侵害，則必須依一般方式通報，即每

項侵害皆須依據第33條進行通報。

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.
雖然GDPR允許在一定程度上之遲延通報，但這不應被視為常態。另需指出，有數個類似侵害須於72小時內通報時，亦可適用包裹通報。

C. Cross-border breaches and breaches at non-EU establishments
跨境侵害以及發生在非設立於歐盟據點之侵害

1. Cross-border breaches
跨境侵害

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that：
在跨境運用[27]個人資料時，侵害可能會影響一個以上成員國之當事人。第33條第1項明確規定，當侵害發生時，控管者應依據GDPR第55條[28]通報權責監管機關。第55條第1項規定：

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."
> 「各監管機關應有權於其成員國領土內依本規則執行指定之職務並行使公權力。」

However, Article 56(1) states：
然而，第56條第1項規定：

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

[27] See Article 4(23).
請參閱第 4 條第 23 項。
[28] See also Recital 122.
請參閱前言第122點。

「在不妨礙第55條之前提下，控管者或受託運用者之主要據點或單一據點的監管機關，為了第60條規定之程序，應足擔任該控管者或受託運用者之跨境運用行為的主責監管機關。」

Furthermore, Article 56(6) states：
此外，第56條第6項規定：

"The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."
「主責監管機關應為控管者或受託運用者執行跨境運用時之唯一溝通對口。」

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.
此意味著在跨境運用中發生侵害，且須通報時，控管者將需通報主責監管機關[29]。因此，在草擬侵害應變計畫時，控管者應評估何監管機關是其所需通報的主責監管機關[30]。這將有助

[29] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.
請參閱 WP29 關於辨別控管者或受託運用者之主責監管機關指引，請查閱：http://ec.europa.eu/newsroom/document.cfm?doc_id=44102。
[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm
所有歐洲國家資料保護機關之聯繫方式列表請查閱：
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

於控管者迅速對侵害做出回應，以履行其依第33條規定之義務。因此，若侵害事件涉及跨境運用，必須通報主責監管機關，該機關之所在地不必是受影響當事人的所在地，或侵害發生地。在通知主責機關時，控管者於適當情況下應說明侵害是否涉及位於其他成員國之據點，以及何成員國內之當事人可能受到該侵害之影響。若控管者對主責監管機關之認定有疑義時，該控管者應至少通知侵害發生地之監管機關。

2. Breaches at non-EU establishments

發生在非設立於歐盟境內機構之侵害

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]：

第3條規範之GDPR地域範圍，包括當其適用於非設立於歐盟境內的控管者或受託運用者所為之個人資料運用的情況。特別是，第3條第2項規定[31]：

> "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> 「本規則適用於非設立於歐盟境內之控管者或受託運用者對位於歐盟境內之當事人所為涉及如下事項之個人資料運用：
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> 對歐盟境內之當事人提供商品或服務，不問是否需要當事人付款;或
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."
>
> 監控當事人於歐盟境內之行為」

Article 3(3) is also relevant and states[32]：

第3條第3項亦與此相關並規定[32]：

[31] See also Recitals 23 and 24
請另參閱前言第 23 點及第 24 點。

[32] See also Recital 25.
請另參閱前言第 25 點。

"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."
「本規則適用於設立在非歐盟境內，但依國際公法而適用成員國法律之領域的控管者所為之個人資料運用。」

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).
因此，當非設立於歐盟境內之控管者符合第3條第2項或第3條第3項要件且有侵害之發生時，仍受第33條和第34條通報義務之拘束。第27條規定當控管者（和受託運用者）有第3條第2項情形時應指定在歐盟境內之代表。在此情形下，WP29建議應通報控管者指定之歐盟境內代表所在成員國之監管機關[33]。同樣，若受託運用者符合第3條第2項要件時，其亦受受託運用者之義務拘束，而與此處特別相關者，即為依據第33條第2項通知控管者侵害之義務。

D. Conditions where notification is not required
無需通報之情形

Article 33(1) makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.
第33條第1項明確規定，「不太可能對自然人權利和自由造成風險」之侵害無需通報監管機關。例如可能是個人資料已經公開可用，且該資料之揭露不會對個人構成可能之風險。此一規定與現行2009/136/EC指令中公眾使用電子通信服務提供者之侵害通報要求不同，該指

[33] See Recital 80 and Article 27.
請參閱前言第 80 點和第 27 條。

令規定所有相關侵害皆須通知權責機關。

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.
在有關侵害通報的03/2014意見中[34]，WP29說明，以最先進演算法加密之個人資料遭受機密性侵害，仍屬個人資料之侵害，因此必須通報。然而，若金鑰之機密性是完整的 – 即金鑰在任何安全侵害中皆未受損，且其產生方式讓任何未經授權存取之人無法透過可用之技術查出 – 則基本上資料是無法解讀的。因此，侵害不太可能對個人產生不利影響，因此亦無需與當事人進行溝通[35]。然而，即使資料被加密，若控管者沒有適當的備份，該資料遺失或變更亦會對當事人產生負面影響。在此情形下，即使資料本身有適當的加密措施，也需要與當事人進行溝通。

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.
WP29亦說明，若個人資料（如密碼）經雜湊與亂數（salted）安全地處理，即雜湊值(Hash值)是以最先進的加密金鑰雜湊函數計算，那麼用於雜湊資料之金鑰將不會在任何侵害中受到損害。且用於雜湊資料之金鑰的產生方式讓任何未經授權存取之人無法透過可用之技術查出。

Consequently, if personal data have been made essentially unintelligible to unauthorised parties

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
WP29，有關侵害通知03/2014意見，請查閱 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf。
[35] See also Article 4(1) and (2) of Regulation 611/2013.
請另參閱 611/2013 規則第 4 條第 1 和 2 款。

and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.
因此，若個人資料對於未授權方而言基本上無法解讀，且資料之副本或備份亦存在，則涉及適當加密之個人資料機密性侵害可能不太需要向監管機關通報。這是因為此種侵害不太可能對個人之權利和自由構成風險，而無高風險之可能也意味著不需要通知當事人。然而，仍須記住，雖然最初可能因為對個人的權利和自由並無可能之風險而無須通報，但這或許會隨著時間的推移而發生變化，並必須重新評估風險。例如，若隨後發現金鑰遭到損害，或加密軟體的漏洞被揭露，則可能仍然需要通報。

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".
此外，應需注意，若侵害發生在加密卻沒有備份之個人資料，則可能存在可用性侵害，而對個人構成風險，因此也許需要通知。同樣，若侵害之發生涉及加密資料的遺失，即使存在個人資料備份，仍可能構成可通報之侵害，具體判定取決於從該備份回復資料所需的時間長短，以及欠缺可用性時對個人之影響。如第32條第1項第c款所述，安全的一個重要因素係「在實體環境或技術性事故中能夠及時回復個人資料可用性和存取之能力」。

Example

示例

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

控管者及其員工所使用的安全加密行動裝置遺失，無需通報監管機關。當加密金鑰保存在控管者安全擁有的範圍內，且遺失之個人資料並非唯一副本，侵害者將無法存取個人資料。此意味著侵害不太可能對相關當事人之權利和自由造成風險。若而後加密金鑰受到損害或加密軟體或演算法有漏洞之情事變得明顯，自然人權利和自由之風險將會改變，因此可能需要通報。

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have “default keys” that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years’ time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

然而，在資料實際上未被安全加密的情況下，若控管者未通報監管機關，則不符合第33條之規範。因此，在選擇加密軟體時，控管者應仔細評估該加密所提供之品質並正確的執行，並了解該加密軟體實際提供的保護層級以及是否適合可能之風險。控管者亦應熟悉其加密產品如何運作之細節。例如，設備可能在關閉後立即加密，但當其處於待機模式時則不加密。某些使用加密的產品具有「內建金鑰」，需要每位用戶更改後才會生效。也有可能該項加密(軟體)在當下會被安全專家認為是足夠的，但幾年後便過時，此意味該加密產品是否

可為資料提供充分加密和適當程度之保護即有疑問。

III. Article 34 – Communication to the data subject
第34條 – 與當事人之溝通

A. Informing individuals
通知當事人

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.
在某些情形下，除了通知監管機關外，控管者尚需向受影響之當事人就侵害進行溝通。

Article 34(1) states：
第34條第1項規定：

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."
> 「於個人資料侵害可能導致自然人權利和自由之高風險時，控管者應與當事人就個人資料侵害進行溝通，不得無故延遲。」

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.
控管者應記住，除非侵害不太可能對個人的權利和自由造成風險，否則向監管機關通報之義務為強制性。此外，若因侵害而可能導致個人之權利和自由面臨高風險時，則必須告知當事人。因此，向個人溝通侵害之門檻高於通報監管機關，所以並非所有侵害皆須與當事人溝通，從而保護其免受不必要的疲勞通知。

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to

provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.
GDPR規定「不得無故遲延」與當事人就侵害所進行之溝通，此意味著應儘快為之。通知當事人的主要目的係提供其有關自我保護所應採取措施之具體資訊[36]。如上所述，依據侵害之性質和所構成之風險，及時溝通將有助於當事人採取措施保護自己免受該侵害的任何負面影響。

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.
本指引的附錄B提供了一份清單列舉侵害何時可能導致當事人高風險之情況，以及控管者因此必須通知受影響個人之情形。

B. Information to be provided
所須提供之資訊

When notifying individuals, Article 34(2) specifies that：
在通知當事人時，第34條第2項規定：

> "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."
>
> 「本條第1項所稱與當事人之溝通，應以清楚簡易之語言描述個人資料侵害的性質，並至少包括第33條第3項第b、c、和d款中提及之資訊與措施。」

According to this provision, the controller should at least provide the following information：
依此規定，控管者至少應提供以下資訊：

- a description of the nature of the breach;
  侵害性質之描述；
- the name and contact details of the data protection officer or other contact point;
  個資保護長或其他聯絡點之姓名(名稱)和聯繫方式；

[36] See also Recital 86.
請另參閱前言第 86 點。

- a description of the likely consequences of the breach; and
  侵害可能之後果的描述；以及
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
  控管者為解決侵害而採取或預計採取之措施的描述，若適當的話，則亦包括為減輕可能之不利影響而採取之措施。

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.
為解決侵害和減輕其可能的不利影響所採取之措施，例如，控管者可聲明，於向相關監管機關通報該侵害後，控管者已獲得有關管理該侵害及減輕其影響之建議。在適當的情況下，控管者亦應向當事人提供具體建議，使其得保護自己免受侵害可能產生之不利後果，例如當存取憑證受損時重置密碼。同樣地，控管者得選擇提供此處要求以外之資訊。

C. Contacting individuals
   聯繫當事人

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).
原則上，應直接與受影響之當事人就相關之侵害進行溝通，除非此種溝通造成不成比例之付出。於此情形下，則應採取公眾溝通或類似措施，使當事人獲得同樣有效方式之通知（第34條第3項第c款）。

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.
在與當事人就侵害進行溝通時，應使用專用訊息，且不應與其他資訊(如定期更新、新聞通

訊或一般標準訊息)一併發送。此有助於使該溝通清晰透明。

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

透明溝通的方法包括如直接傳送訊息（例如，電子郵件、簡訊、直接訊息）、明顯的網站橫幅式廣告或通知、郵政通訊以及在印刷媒體中明顯的廣告。僅於新聞稿或在公司部落格上通知並非屬與當事人溝通侵害的有效方式。WP29建議控管者應選擇一種可使資訊傳達給所有受影響當事人之機會最大化。依據具體情況，這可能意味著控管者得採取多種溝通方式，而非僅使用單一接觸管道。

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

控管者可能亦需要確保溝通係以適當的替代形式和相關語言為之，以確保當事人能夠理解所提供之資訊。例如，在與當事人就侵害進行溝通時，使用和接收者在從前正常業務過程中所使用之語言通常是合適的。然而，若受侵害影響之當事人係控管者先前未曾與其進行過互動之個人，或特別是那些居住在控管者所在地以外之其他成員國或其他非歐盟國家之個人，在考量所需之資源，以當地國家之語言進行溝通是可接受的。關鍵在於協助當事人了解侵害之性質以及可採取保護自己之措施。

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the

breach as this channel could also be used by attackers impersonating the controller.
控管者最適合決定最適當的連繫管道，以與當事人就侵害進行溝通，特別是當控管者與客戶間有經常之互動情形。然而，顯然地，控管者應謹慎使用已受侵害之連繫管道，因為攻擊者亦可能冒充控管者使用該管道。

At the same time, Recital 86 explains that：
同時，前言第86點說明：

> "Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."
> 「此種與當事人之溝通應儘快在合理可行的情況下進行，且與監管機關密切合作，尊重監管機關或其他相關機關如執法機關提供之指導。例如，需降低損害之立即風險即須立刻與當事人溝通，而需實施適當措施以對抗持續的或類似的個人資料侵害則可使較長的溝通時間正當化。」

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.
因此，除了如何依據第34條通知當事人之建議外，控管者亦可能希望與監管機關連繫並諮詢有關發送適當訊息及聯繫當事人之最適方式的建議。

Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.
與前言第88點中之建議相連結，即侵害之通知應「考量執法機關的合法正當利益，當早期揭露可能會對個人資料侵害情形之調查造成不必要之妨礙」。這可能意味著在特定正當情形下，並依據執法機關之建議，控管者與受影響當事人就侵害之溝通得予延遲，直到不會

損害該調查為止。然而，其後仍需迅速通知該當事人。

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).
當儲存之資料不足以聯繫當事人，控管者則無法向該當事人就侵害進行溝通，在此特殊情形下，控管者應在溝通合理可行時，立即通知當事人(例如，當事人行使其第15條權利以近用個人資料並向控管者提供必要的附加資訊以便聯繫時)。

D. Conditions where communication is not required
不須溝通之情形

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are：
第34條第3項規定不須向當事人通知侵害的三種情形，包括：

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
  在侵害發生前，控管者對個人資料之保護已採取適當的技術性與組織性措施，特別是使未獲授權存取之人無法解讀個人資料之措施。例如，可能包括使用最先進之加密或透過代碼化(tokenization)來保護個人資料。

- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
  在侵害發生後，控管者立即採取措施確保個人權利和自由之高風險已不再可能實現。例如，依據案件具體情況，在存取個人資料者進行任何操作之前，控管者或許已立即辨別出並對其採取行動。仍須適當考量任何保密性之侵害可能的結果，

同樣地，此須取決於相關資料之性質。

- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.
  若聯繫當事人可能造成不符比例之付出[37]，或因侵害而遺失聯繫方式或從一開始便不知悉聯繫方式。例如，統計辦公室的倉庫被淹沒，而包含個人資料之文件僅以紙本形式儲存。控管者必須採取公眾溝通或類似措施替代，以同樣有效之方式通知當事人。在不成比例之付出情況下，控管者可設想以技術性之安排，依需求提供侵害之資訊，這對可能受侵害影響卻無法聯繫之當事人有所助益。

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.
依據課責原則，控管者應要能夠向監管機關證明其符合一種或多種之情形[38]。仍須記住，雖然因為對自然人的權利和自由無風險之存在，最初也許不需要通知，但這或許會隨著時間的推移而發生變化，並必須重新評估風險。

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850
請參閱 WP29 關於透明化之指引，該指引將考量不成比例付出之議題，請查閱：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850。
[38] See Article 5(2)
請參閱第 5 條第 2 項。

employing its available powers and sanctions.
若控管者決定不向當事人就侵害進行溝通，第34條第4項說明，當監管機關認為該侵害可能會對個人造成高風險，監管機關可要求控管者為之。又或監管機關認第34條第3項之要件已被滿足，在此情形下則不需要通知當事人。若監管機關認為不通知當事人之決定並無充分依據，得考量採取其可使用之權力和裁罰。

IV. Assessing risk and high risk
風險和高風險之評估

A. Risk as a trigger for notification
風險為觸發通知之要件

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances：
雖然GDPR採用了侵害通知之義務，但該義務並非適用於所有情況：

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
  除非侵害不太可能對個人之權利及自由造成風險，否則必須通報權責監管機關。

- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.
  只有在可能對其權利和自由造成高風險之情況下才會觸發與當事人就侵害進行溝通之義務。

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this： firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.
這表示一旦知悉侵害，控管者不僅應該設法控制事故，還應該評估該事件可能導致之風險，這一點非常重要。此包含兩項重要原因：第一，瞭解對個人影響之可能性和潛在嚴重程度將有助於控管者採取有效措施來控制和解決侵害；第二，這將有助於決定是否需通報監管機關，並在必要時通知相關當事人。

As explained above, notification of a breach is required unless it is unlikely to result in a risk to

the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

如上所述，除非不太可能對個人之權利及自由造成風險，否則必須通知侵害，且需要向當事人就侵害進行溝通之關鍵觸發要件為對個人之權利和自由造成高風險之可能。此種風險存在於當侵害可能導致資料被破壞之當事人遭受人身、財物或非財物的損害。損害之示例包括歧視、冒用身分或詐欺、財務損失和聲譽受損。當侵害涉及揭露種族或民族血統、政治觀點、宗教或哲學信仰或公會會員資格之個人資料，或包括基因資料、有關健康之資料或有關性生活之資料，或前科及犯罪或相關安全措施，此時應被認定有損害發生之可能[39]。

B. Factors to consider when assessing risk
風險評估考量之要件

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

GDPR前言第75點和第76點建議，通常在評估風險時，應考量當事人之權利和自由所受風險的可能性和嚴重性。前言進一步指出，風險應在客觀評鑑基礎上為之。

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

---

[39] See Recital 75 and Recital 85.

請參閱前言第75點及前言第85點。

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

請參閱 WP 關於 DPIA 之指引：http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。

應該注意到，評估因侵害而對個人權利和自由所造成之風險與個資保護影響評估(DPIA)[40]中考量之風險所關注的重點不盡相同。DPIA同時考量按計畫進行資料運用之風險，以及若發生侵害之風險。在考量潛在的侵害時，DPIA概括性的著重在發生此類情形之可能性，以及對當事人可能發生之損害；易言之，這是對假設事件之評估。就實際之侵害而言，由於事件已經發生，因此完全著重於侵害對個人造成之影響。

Example

示例

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

DPIA建議，預計使用特定安全軟體產品來保護個人資料是一種合適的措施，以確保因運用程序對個人造成之風險有適當的安全層級。然而，若隨後始知悉漏洞，這將改變該軟體控制受保護的個人資料風險之合適性，因此作為進行中的DPIA的一部分，須重新評估。

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

產品中之漏洞隨後被利用，並發生侵害。控管者應評估侵害之具體情況、受影響之資料、對個人的潛在影響程度、以及該風險實現之可能性。

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]：

因此，在評估因侵害導致的個人風險時，控管者應考量侵害之具體情況，包括潛在影響的嚴重程度以及該情況發生之可能性。因此，WP29建議評估應考量以下標準[41]：

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR.
See http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
611/2013 規則第 3.2 條為電子通訊服務業就侵害通知應考量之要素提供指導，該指導可能對 GDPR 下關於通知之義務有所助益。請查閱:
http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF。

- The type of breach
  侵害之類型

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.
已發生之侵害類型可能會影響對個人造成風險之程度。例如，在機密性之侵害中，醫療資訊被揭露予未授權之人對個人所造成之後果，應與個人詳細醫療資料遺失且無法再使用之情況不同。

- The nature, sensitivity, and volume of personal data
  個人資料之性質、敏感性和數量

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.
當然，在評估風險時，關鍵因素是受侵害影響的個人資料之類型和敏感性。通常，資料越敏感，被影響之當事人受到傷害之風險就越高，但仍應考量已可使用的有關當事人的其他個人資料。例如，在一般情況下，揭露個人姓名和地址不太可能造成實質的損害。然而，若將養父母之姓名和地址透露予親生父母，則對養父母和子女造成之後果可能非常嚴重。

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.
涉及健康資料、身分證明文件或財務資料（如信用卡詳細資訊）之侵害本身皆可造成傷害，若將資料一併使用，則可能會被用於冒用身分。個人資料之組合通常比單項個人資料更為敏感。

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have

requested that their deliveries be stopped while on holiday would be useful information to criminals.
某些類型的個人資料最初可能相對無害，然而，應仔細考量該資料可能揭露受影響個人之程度。一份接受定期遞送的客戶列表可能並非特別敏感，但是同樣的資料，若是關於客戶要求在休假期間停止遞送，對於犯罪分子來說則是有用之資訊。

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.
同樣的，少量卻高度敏感之個人資料可能對個人產生重大影響，且大量的詳細資料可能揭露關於該個人更大範圍的資訊。此外，當侵害影響許多當事人之大量個人資料時，該侵害會對相對應之大量個人產生影響。

- Ease of identification of individuals
  識別個人之容易度

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.
需考量的一項重要因素為，對能夠存取受侵害個人資料之一方而言，其可識別特定個人或以資料與其他資訊進行對照以識別個人之容易程度為何。依據具體情況，也許可直接從受侵害之個人資料進行識別，而無需特殊研究便可辨別個人身分，又或將個人資料與特定個人對照也許非常困難，但在某些條件下仍有可能為之。從受侵害之資料中可能直接或間接識別個人，能否識別也可能與侵害之具體背景及相關個人詳細資訊的公開可得性相關。此處可能與機密性和可用性之侵害更為相關。

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data

subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.
如上所述，受到適當加密程度保護的個人資料對於沒有解密金鑰之未經授權人而言是無法解讀的。此外，適當採用假名化(第4條第5款將其定義為「運用個人資料之方式，即個人資料在不使用額外資訊時，無法識別出特定之當事人，且該額外資訊已被分開保存，並以技術性與組織性措施確保該個人資料無法顯示已識別或可識別之自然人」)亦可降低在發生侵害時識別個人之可能性。然而，單獨使用假名化技術不能被認作使資料無法解讀。

- Severity of consequences for individuals
  對當事人造成之嚴重後果

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.
依據侵害所涉及個人資料之性質，例如特殊類別之資料，對個人造成的潛在損害可能格外嚴重，特別是在該侵害會導致身分遭冒用或詐欺、身體傷害、心理困擾、羞辱或損害名譽之情況時。若侵害涉及弱勢群體之個人資料，可能會使他們置身於更大的損害風險中。

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the

controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

控管者是否知悉個人資料掌握在意圖不明或可能為惡意之人的手中，會影響潛在風險之程度。當向如第4條第10款所定義之第三方或其他錯誤之接收者揭露個人資料時，則可能會有機密性侵害。例如，可能發生個人資料意外傳送至組織的錯誤部門或常用的供應商。控管者可能要求接收者返還或安全地銷毀所接收之資料。在此二情形下，因控管者與錯誤的接收者有持續性之關係，並可能知悉其程序、歷史和其他相關細節，因此可認定該接收者為「可信任的」。也就是說，控管者對該接收者可能具有一定程度的確信，可以合理期待該接收者不會閱讀或存取錯誤發送之資料，並遵守返還該資料之要求。即使已存取了資料，控管者仍可能信任接收者不會對該資料採取任何進一步之操作，並立即將資料返還給控管者且與其合作回復資料。在此情形下，這可能會成為控管者在侵害發生後進行風險評估中的要素之一：接收者係可信任的事實可能會消除侵害後果之嚴重性，但並不意味著沒有侵害之發生。然而，這可能會去除個人風險的可能性，因此不再需要通報監管機關或受影響之當事人。同樣地，這將取決於具體個案情況。儘管如此，作為保存侵害記錄之一般義務的一部分，控管者仍必須保留侵害之相關紀錄（請參閱下文第V節）。

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

另應考量對個人造成後果之持續性，若影響為長期性，則可能會認為衝擊較大。

- Special characteristics of the individual
  當事人之特點

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

侵害可能會涉及有關兒童或其他弱勢者之個人資料，使其面臨更高之危險風險。尚存在關於當事人之其他因素可能影響侵害對其造成衝擊之程度。

- Special characteristics of the data controller
  資料控管者之特點

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
控管者的性質和角色與其活動，可能會影響因侵害而對個人造成風險之程度。例如，醫療機構運用特種個人資料，意味著若該個人資料遭受侵害，相較於報紙的郵寄名單而言，將會對當事人造成更大之風險。

- The number of affected individuals
  受影響當事人之數量

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.
侵害可能影響一個人、少數人或數千人。一般來說，受影響當事人越多，侵害造成的衝擊就越大。然而，依個人資料之性質與其受損害之情況，侵害甚至可能僅對一個人產生嚴重的影響。同樣地，關鍵是要考量對受影響個人造成衝擊之可能性和嚴重性。

- General points
  一般要點

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.
因此，在評估可能因侵害而造成之風險時，控管者應同時考量對當事人權利和自由潛在影響之嚴重程度以及該影響發生之可能性。顯然地，若侵害之後果越嚴重，風險就越高，同樣地，當發生的可能性越大，風險也會提高。若有疑問，控管者應謹慎行事並進行通知。

附錄B提供了一些不同類型之侵害所涉及當事人風險或高風險的有用範例。

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].
歐盟網路和資訊安全局（ENISA）就評估侵害嚴重性之方式提出了建議，這對控管者和受託運用者在設計侵害管理應變計畫時也許有所助益[42]。

V. Accountability and record keeping
歸責和紀錄之保存

A. Documenting breaches
記錄侵害事件

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains：
無論侵害是否需要通報監管機關，控管者必須留存所有侵害之紀錄，如第33條第5項所述：

> "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."
> 「控管者應記錄任何個人資料侵害事件，包括與個人資料侵害相關之事實、其影響和所採取之補救措施。該紀錄應使監管機關得以確認是否符合本條。」

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

---

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity
ENISA，關於評估當事人資料侵害嚴重性方法之建議，請查閱：https://www.enisa.europa.eu/publications/dbn-severity。

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.
控管者可以選擇將記錄侵害作為其依據第 30 條保存運用活動紀錄之一部分。若可清楚識別與侵害相關之資訊，並可根據要求提取，則不需要分別登記。

這可連結至GDPR第5條第2項所規範之課責原則。記錄不須通報之侵害的目的與應通報之侵害的目的一樣，與第24條之控管者義務相關，且監管機關可要求查看該紀錄。因此，無論是否需要通報，鼓勵控管者建立內部侵害登記制度[43]。

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

雖然係由控管者決定在記錄侵害時所使用之方法和結構，但就可記錄之資訊而言，有適用於所有情況之關鍵要素。依據第33條第5項之規定，控管者需記錄關於侵害之詳細資訊，其中應包括侵害之原因、發生之事件以及受影響之個人資料。亦應包含侵害之影響與後果，以及控管者所採取之補救措施。

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.

GDPR並未規定此類紀錄的保留期間。若此類紀錄包含個人資料，則控管者有責任依據與個人資料運用有關之原則[44]決定適當的保留期限，並符合合法運用之要件[45]。控管者需依據第33條第5項保留紀錄，當監管機關要求時，做為遵循該條規定或符合課責原則之證據。顯然地，若紀錄本身不包含個人資料，則不適用GDPR的儲存限制原則[46]。

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers

---

[44] See Article 5.
請參閱第5條。
[45] See Article 6 and also Article 9.
請參閱第6條及第9條。
[46] See Article 5(1)(e).
請參閱第 5 條第 1 項第 e 款。

the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.
除這些細節外，WP29亦建議控管者記錄其就侵害所做決定之理由。特別是，若未通報該項侵害，該決定之正當性應予記錄。這應包括控管者認為該侵害不太可能對個人權利和自由造成風險之原因[47]。或者，若控管者認為已符合第34條第3項中之任何要件，則應能夠提供適當證據證明之。

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.
當控管者確實向監管機關通報侵害，但該通報是遲延的，則控管者必須能夠提供遲延之理由；與此相關之紀錄有助於彰顯該遲延通報係正當且非過度的。

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.
當控管者向受影響之當事人就侵害進行溝通時，關於該侵害(相關內容)應透明，並以且有效之方式進行。因此，藉由保留此類溝通之證據，將有助於控管者彰顯其課責性和合規。

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.
為協助遵循第33條和第34條之規定，若控管者和受託運用者皆執行通報程序記錄，列出在偵測到侵害後所應遵循之流程，包括如何控制、管理和修復該事件，以及評估風險和通報該侵害。就此，可展現其遵循GDPR，並可能有助於說明員工已被告知此類程序和機制之存在，並知悉如何應對侵害之發生。

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with

[47] See Recital 85
請參閱前言第 85 點。

Article 83.
另應注意，未妥善記錄侵害將使監管機關得依據第58條行使其權力，及/或依據第83條處以行政罰鍰。

B. Role of the Data Protection Officer
個資保護長之角色

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.
控管者或受託運用者可依據第37條之要求或出於自願性的良好實踐指派個資保護長（DPO）[48]。GDPR第39條規定一些DPO之強制性任務，但於適當情形下，並不妨礙控管者分配其他任務予DPO。

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.
DPO的強制性任務中與侵害通報特別相關者，包括向控管者或受託運用者提供資料保護建議和資訊、監控對GDPR的遵循及提供與DPIA相關之建議。DPO亦須與監管機關合作，並作為監管機關和當事人之聯絡點。另須注意，第33條第3項b款要求於向監管機關通報侵害時，控管者應提供其DPO或其他聯絡點之名稱和詳細聯繫方式。

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.
就侵害之記錄而言，控管者或受託運用者可能希望獲得DPO就關於該紀錄的結構、設置和管理方面之意見。DPO還可能被額外指派負責維護這些紀錄之任務。

These factors mean that the DPO should play an key role in assisting the prevention of or

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
請參閱 WP 有關 DPO 之指引文件: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083。

preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

這些要素意味著DPO應透過提供建議和監督合規性，在協助防止侵害或侵害之因應準備、與侵害期間(即通報監管機關時)及任何後續監管機關的調查期間，扮演關鍵角色。有鑑於此，WP29建議應迅速通知DPO侵害之存在，並使其參與整個侵害管理和通報之程序。

VI. Notification obligations under other legal instruments
其他法律文件下之通報義務

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following：

除了依據GDPR通報和溝通侵害之義務外，控管者亦須知悉依據其他可能適用的相關法律就通報安全事件之任何要求，以及是否可能也同時要求他們就個人資料侵害之情事通報監管機關。該要求可能因成員國而異，但其他法律文件規定之通報要求及其如何與GDPR相互關連之示例如下：

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

(EU)910/2014 關於歐盟內部市場電子交易之電子識別和信賴服務規則（eIDAS規則）[49]。

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

eIDAS規則第19條第2項要求信賴服務提供者，當其遭受之安全侵害或信賴喪失會對所提供

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG。

之信賴服務或其所保存之個人資料產生重大影響時，應通報其監管部門。而在適用之情形下 - 即若此類侵害或損失亦屬GDPR下之個人資料侵害時 - 信賴服務提供者亦應通報監管機關。

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

（EU）2016/1148關於跨歐盟網路與資訊系統高度共同安全措施指令（NIS指令）[50]。

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

NIS指令第14條和第16條要求基本服務運營商和數位服務提供者向其權責機關通報安全事故。依據NIS前言第63點[51]，安全事故通常會包含個人資料之侵害。雖然NIS要求權責機關和監管機關合作並交換資訊，但若該類事件是/或成為GDPR下之個人資料侵害，則該運營商和/或提供者可能被要求與NIS要求之事故通報分開，另行通報監管機關。

Example

示例

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

若侵害事件包括個人資料侵害，雲端服務提供者依據NIS指令通報侵害時，可能亦需通知控管者。同樣的，在侵害發生時，信賴服務提供者依據eIDAS通報侵害事件時，亦有可能被要求通報相關個人資料保護機關。

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG。

[51] Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*
前言第 63 點:「*在許多案例中，個人資料會因事故而受到損害。在此情形下，權責機關和資料保護機關應合作並交換所有相關事項之資訊，以解決因事故而導致的任何個人資料侵害。*」

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).
  2009/136/EC指令（公民權利指令）和 611/2013規則（侵害通知規則）。

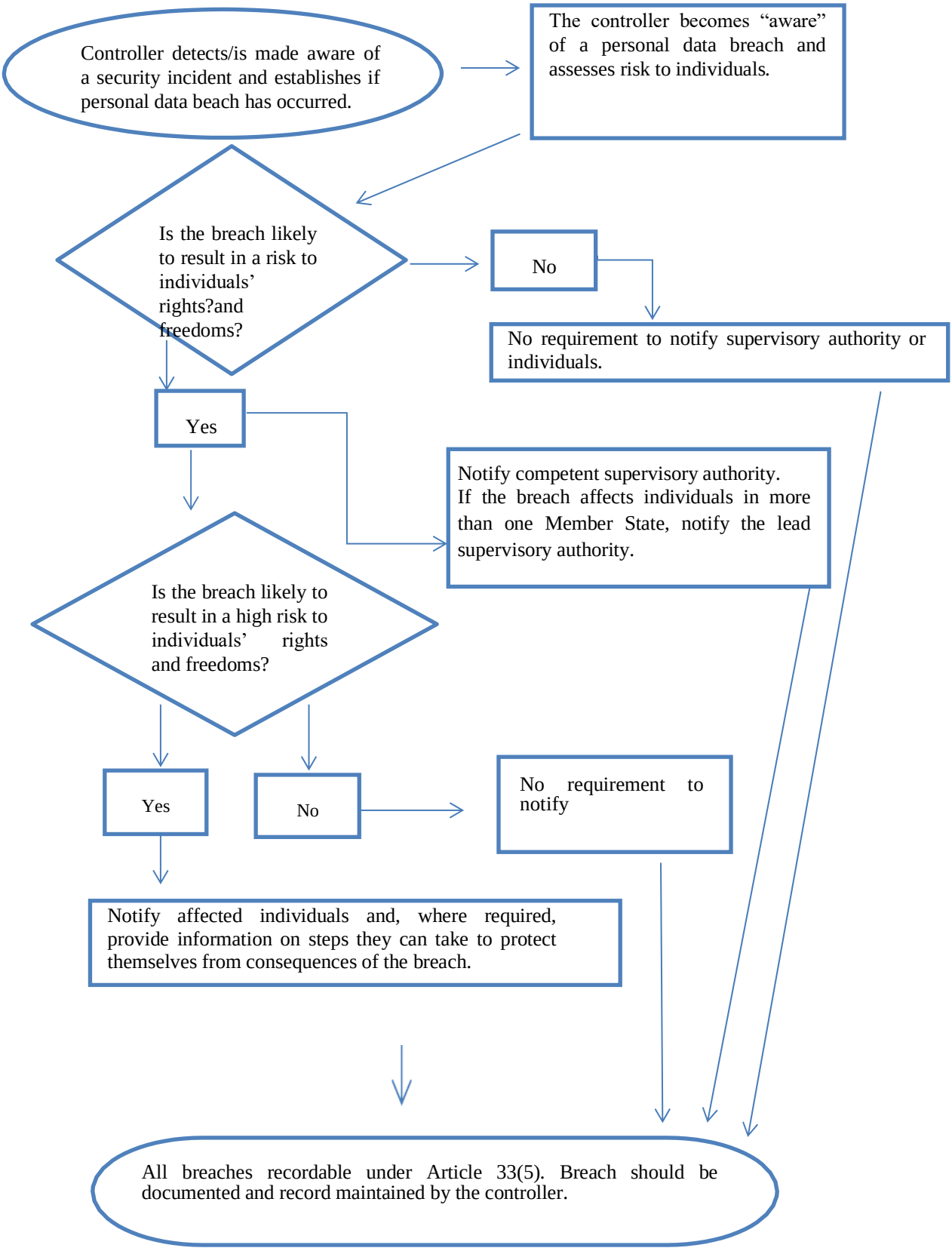
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52]must notify breaches to the competent national authorities.
在2002/58/EC[52]指令中所指之公眾電子通信服務提供者必須將侵害通報權責國家機關。

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.
控管者亦應知悉於其他可適用制度下之任何額外法律、醫療或專業之通知責任。

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, seehttps://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
2017 年 1 月 10 日，歐盟執委會提出了一項關於隱私權和電子通訊規則，此將取代 2009/136/EC 指令並刪除通知之要求。然而，在歐洲議會批准該提案前，現有之通知要求仍屬有效，請參閱:
https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications。

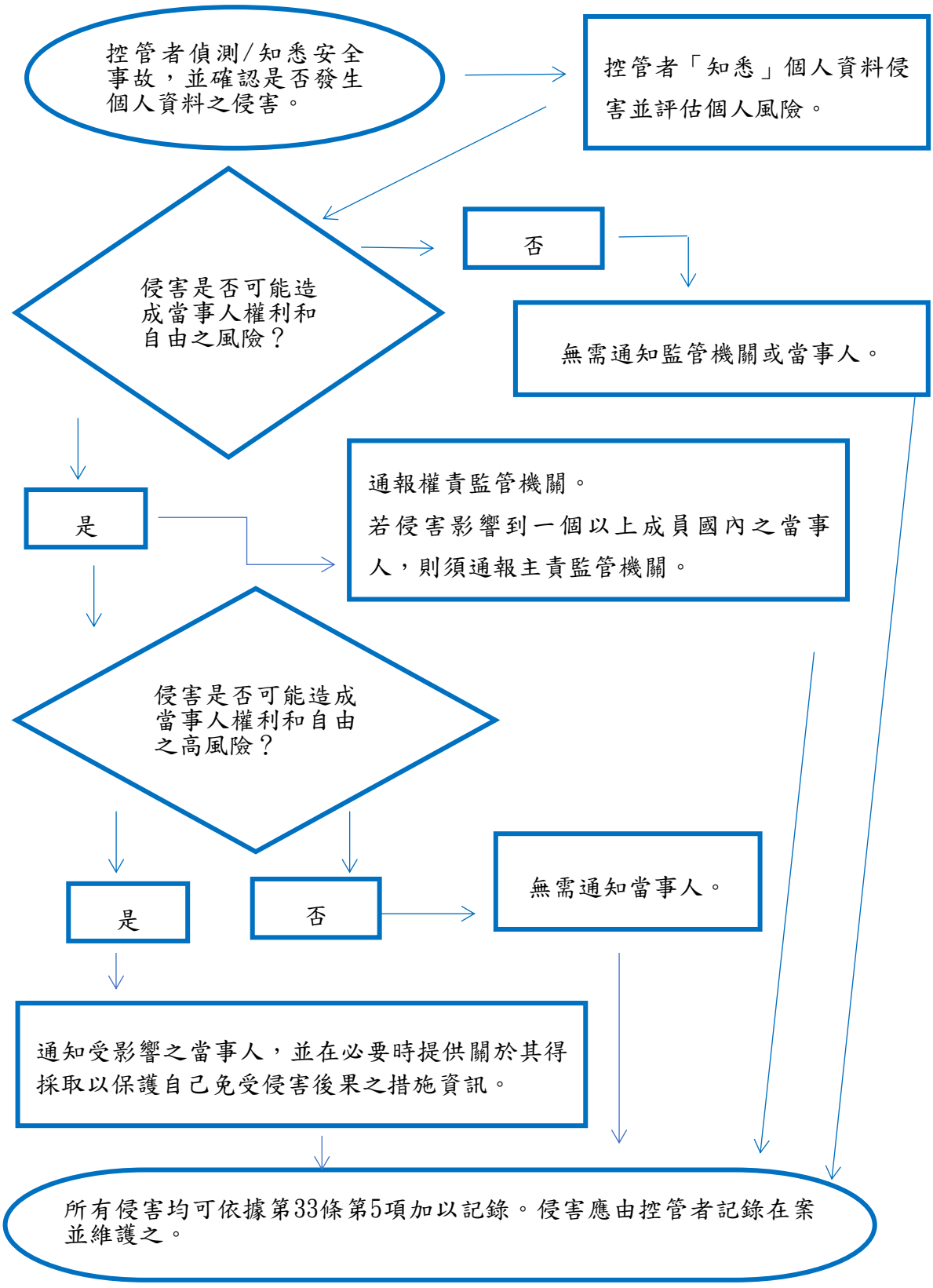
VII. Annex

A. Flowchart showing notification requirements



VII. 附錄

A. 通知要求流程圖



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.

iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a

			digital service provider.
vii. A website hosting company acting as data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigations the affected controllers should be reasonably confident as to whether each has suffered a breach and thereof is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individual they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to：" or "cc：" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist)	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

	or if other factors present high risks (e.g. the mail contains the initial passwords).		

B. 個人資料侵害示例及應通報(知)之對象

以下非完全列舉之示例將協助控管者決定在不同的個人資料侵害情況下是否需要進行通知。這些示例也可能有助於區分對個人權利和自由之風險及高風險。

示例	是否通報監管機關？	是否通知當事人？	注意事項/建議
i. 控管者將個人資料之備份檔案儲存在加密的USB智能儲存裝置上。該裝置因竊盜闖入而遭偷竊。	否。	否。	只要資料是以最先進的演算法進行加密、資料備份仍存在該特定金鑰未受到損害，且資料可於適當時機回復時，則可能不屬於需要通報之侵害。 然而，若其後遭受損害，則需要通報。
ii. 控管者維護一個線上服務。由於對該服務的網路攻擊，致使當事人的個人資料外洩。 該控管者僅在歐盟單一成員國境內擁有客戶。	是，若對當事人可能產生後果，應通報監管機關。	是，依據受影響個人資料之性質以及對當事人權利可能造成後果之嚴重性，通知該當事人。	
iii. 控管者電話服務中心短暫停電幾分鐘，意味著客戶無法致電控管者並存取其紀錄。	否。	否。	此非屬須通知之侵害，但仍屬於第33條第5項規定下可記錄之事故。控管者應保存適當之記錄。
iv. 控管者遭受勒索軟體攻擊，導致所有資料皆被加密。無可用之備份，亦無法回	是，若可能對當事人產生後果，需通報監管機構，因其屬於可用性喪失之侵害。	是，依據受影響個人資料之性質以及無法獲取資料可能產生之影響，以及	若有可用之備份且資料可適時回復，則不需要通報監管機關或當事人，因此處並無永久

復資料。在調查中發現，很明顯勒索軟體的唯一功能是加密資料，且系統中不存在其他惡意軟體。		其他可能之後果，通知當事人。	的可用性或機密性之損失。 然而，若監管機關透過其他方式知悉該事故，得考慮進行調查，以評估是否符合第32條中更廣泛之安全要求。
v. 某人致電給銀行的電話服務中心告知資料侵害事件。該個人收到其他人的月結單。 控管者進行了簡短的調查（即在24小時內完成），並合理確信已發生個人資料之侵害，以及是否存在系統性缺陷，可能意味著其他人受到或可能受到影響。	是。	若存在高風險且明顯地並無其他人受到影響，則僅需通知受影響之當事人。	若在進一步調查後發現有更多人受到影響，則必須向監管機關更新通報，且若對其他人存在高風險時，控管者需要採取額外步驟，對他人進行通知。
vi. 控管者經營一個網路賣場，並在多個成員國皆擁有客戶。該賣場遭受網路攻擊，且攻擊者在網路公布用戶名稱、密碼和購買歷史記錄。	是，若涉及跨境運用，通知主責監管機關。	是，因其可能造成高風險。	控管者應該採取行動，例如透過強制重置受影響帳戶之密碼，以及其他降低風險之措施。 控管者尚應考量任何其他通知義務，例如：作為NIS指令中數位服務提供者之義務。

vii. 擔任資料受託運用者之網站託管公司發現控制用戶授權之程式碼有錯誤。該錯誤之影響意味著任何用戶皆可存取任何其他用戶的帳戶詳細資訊。	作為受託運用者，網站託管公司必須通知其受影響之客戶（控管者），不得無故遲延。 假設網站託管公司已自身進行了調查，受影響之控管者應對是否遭受侵害有合理之確信，因此一經託管公司（受託運用者）通知，即可被視為「知悉」。控管者因而必須通報監管機關。	若對當事人沒有造成高風險之可能，則不需通知。	網站託管公司（受託運用者）必須考量任何其他通知義務（例如，作為NIS指令中數位服務提供者之義務）。 若無證據表明此錯誤被其任何控管者利用，則可能沒有發生須通知之侵害，但仍可屬於係可記錄之侵害，或是屬於第32條中不合規之情形。
viii. 由於網路攻擊，醫院病歷在30小時內無法使用。	是，基於對患者健康與隱私之高風險，醫院有義務通報。	是，須通知受影響之當事人。	
ix. 大量學生的個人資料被錯誤地發送到有1000多個收件人之錯誤郵件列表。	是，須通報監管機關。	是，依據所涉及個人資料之範圍和類型以及可能後果之嚴重程度，通知當事人。	
x.行銷電子郵件將收件人郵件放置在正本收件人「to：」或副本收件人「cc：」中，因此每個收件人都可看到其他收件人之電子郵件地址。	是，若大量當事人受到影響；或若敏感資料遭揭露（例如心理治療師之郵件列表）；或其他存在高風險之因素（例如包含原始密碼之郵件），通報監管機關則可能是強制性的。	是，依據所涉及個人資料之範圍和類型以及可能後果之嚴重程度，通知當事人。	若未揭露敏感資料且僅有少量電子郵件地址遭揭露，則可能不需要通知。

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN

WP 243 rev.01

Guidelines on Data Protection Officers ('DPOs')
關於個資保護長（DPO）之指引

Adopted on 13 December 2016

As last Revised and Adopted on 5 April 2017

2016年12月13日通過

2017年4月5日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 05/35.
由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
網址：http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,
having regard to Articles 29 and 30 thereof,
having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日之第95/46/EC號指令而設立，
基於該指令第29條及第30條，
基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Table of content

目錄

1 Introduction 導言

The General Data Protection Regulation ('GDPR'),[1] due to come into effect on 25 May 2018, provides a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR.
訂於2018年5月25生效之「一般資料保護規則（General Data Protection Regulation，GDPR）」[1]提供了歐洲一套現代化、以課責性為基礎之資料保護遵循架構。個資保護長（DPO）將會是此一新法律架構下，許多組織中推動遵循GDPR規範之核心。

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO.2 This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.
於GDPR規範下，對某些控管者及受託運用者而言，必須指派一名DPO[2]。此規範適用於所有公務機關或機構（無論其運用何種資料），及其他核心業務為大規模對個人進行系統性監控，或大規模運用特種個人資料之組織。

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.
即使在GDPR未明確要求必須指派DPO之情況下，各組織有時也可能認為設置DPO有其

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016). The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement.
2016年4月27日歐洲議會與歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，並廢除第95/46/EC號指令，制定歐盟第2016/679號規則（一般資料保護規則）（OJ L 119, 4.5.2016）。GDPR與歐洲經濟區相關，並將在納入歐洲經濟區協議後適用。

[2] The appointment of a DPO is also mandatory for competent authorities under Article 32 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89 – 131), and national implementing legislation. While these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions.
歐洲議會與歐盟理事會2016年4月27日通過之歐盟第2016/680號指令第32條，係權責機關為預防、調查、發現或起訴犯罪或執行刑罰之目的所為個資運用中對自然人之保護、確保該資料自由流通，並廢除理事會第2008/977/JHA號架構決定（OJ L 119, 4.5.2016, p. 89 – 131），以及各國之執行法規，主管機關指派DPO亦為強制規定。此指導原則雖聚焦於GDPR下規範之DPO，但亦可為第2016/680號指令中，近似條文規範DPO事宜之參照。

益處而自願指派。第29條資料保護工作小組（下稱WP29）亦鼓勵此自願性質之努力。

The concept of DPO is not new. Although Directive 95/46/EC[3] did not require any organisation to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years.
DPO並非新的概念。95/46/EC指令[3]雖未要求任何組織須指定DPO，但此種指派DPO之作法已於若干會員國發展多年。

Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.[4] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).
於GDPR通過前，WP29即主張DPO為課責性之基石，且指定DPO可促進法遵，並進一步成為企業之競爭優勢[4]。除透過採用課責性工具（如推動個資保護影響評估及實施或推動稽核作業）促進法遵外，DPO亦為相關利害關係人（例如：監管機關、當事人及組織內之業務單位）間之中介者。

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.
如未遵循GDPR，並不歸責於DPO個人。GDPR清楚規定應由控管者或受託運用者確保並得以證明依其規範執行運用（第24條第1項）。遵循資料保護規範，係控管者或受託運用者之責任。

The controller or the processor also has a crucial role in enabling the effective performance of

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
1995年10月24日歐洲議會與歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，所制定之歐盟第95/46/EC號指令（OJ L 281, 23.11.1995, p. 31）。
[4] See http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf
詳參 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively.
控管者或受託運用者於使DPO有效執行任務上，亦扮演重要角色。指定DPO僅是第一步，DPO亦須被賦予充足之自主性及資源方可有效執行任務。

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of these guidelines is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States. The WP29 will monitor the implementation of these guidelines and may complement them with further details as appropriate.
GDPR將DPO視為嶄新的資料治理體系中之關鍵角色，並規定了DPO指派之條件，及其職位與任務。本指引之目的在於釐清GDPR之相關條文，以協助控管者及受託運用者遵循該法，亦在於協助DPO扮演其角色。本指引亦以部分歐盟成員國之經驗為基礎，就最佳做法提出建議。WP29將持續留意此指引之執行情形，並可能於後續適時補充更多細節。

2 Designation of a DPO
DPO之指派

2.1. Mandatory designation
強制指派

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:[5]
GDPR第37條第1項要求在三種情形下必須指派DPO[5]：

a) where the processing is carried out by a public authority or body;[6]
資料運用係由公務機關或機構為之；[6]

b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or

[5] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well.
此處應留意，依據第37條第4項規定，歐盟或會員國法律可能要求於其他情形下，亦須指派DPO。
[6] Except for courts acting in their judicial capacity. See Article 32 of Directive (EU) 2016/680.
除法院行使其司法功能外。參照歐盟第2016/680號指令第32條。

控管者或受託運用者之核心業務，包含需經常性、系統性對當事人進行大規模監控之運用作業；或

c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data[7] or[8] personal data relating to criminal convictions and offences.[9]
控管者或受託運用者之核心業務，包含大規模運用特種資料[7]或[8]與刑事前科及犯罪相關之個人資料[9]。

In the following subsections, the WP29 provides guidance with regard to the criteria and terminology used in Article 37(1).
WP29於以下小節就第37條第1項之標準及術語提供指導。

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.[10] This analysis is part of the documentation under the accountability principle. It may be required by the supervisory authority and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services that might fall within the cases listed in Article 37(1).
除組織顯無須指派DPO外，WP29建議控管者及受託運用者記錄其決定是否要指派DPO所進行之內部分析，以證明相關因素均已妥善納入考量[10]。此分析為課責性原則下證明文件之一部分。監管機關可能會要求提供該項分析，必要時並應更新該項分析，例如控管者或受託運用者從事之新業務或提供之新服務可能落入第37條第1項所列情形時。

When an organisation designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been

[7] Pursuant to Article 9 these include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
依據第9條規定，此類別包括種族或民族血統、政治觀點、宗教或哲學信仰、公會會員資格、為識別自然人而運用之基因資料及生物辨識資料、健康相關資料或自然人之性生活或性傾向相關資料。
[8] Article 37(1)(c) uses the word '*and*'. See Section 2.1.5 below for explanation on the use of '*or*' instead of '*and.*'
第37條第1項第c款之用字為「及」。參照本指引第2.1.5節以下關於使用「或」而不用「及」之說明。
[9] Article 10.
第10條。
[10] See Article 24(1).
參照第24條第1項。

mandatory.
當一組織自願指派DPO時，其指派、職位及任務即與強制指派同樣適用第37條至第39條之要件。

Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data. In this case it is important to ensure that there is no confusion regarding their title, status, position and tasks. Therefore, it should be made clear, in any communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a data protection officer (DPO). [11]
法律上無義務也無意自願指派DPO之組織，由其員工或外部顧問執行個資保護之相關任務，亦無不可。在此情形下，重要的是確保該人員之職稱、地位、職位及任務不得混淆。因此，於公司內部及其與資料保護機關、當事人及一般大眾間之溝通中，該員或顧問的職稱不得為DPO[11]。

The DPO, whether mandatory or voluntary, is designated for all the processing operations carried out by the controller or the processor.
無論強制或自願性指派之DPO，係為控管者或受託運用者所有的資料運用作業而指派。

2.1.1 'PUBLIC AUTHORITY OR BODY'
公務機關或機構

The GDPR does not define what constitutes a '*public authority or body'*. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[12] In such cases, the designation of a DPO is mandatory.

[11] This is also relevant for chief privacy officers ('CPO's) or other privacy professionals already in place today in some companies, who may not always meet the GDPR criteria, for instance, in terms of available resources or guarantees for independence, and, if they do not, they cannot be considered and referred to as DPOs.
此規定亦涉及首席隱私長（chief privacy officers，CPO）或其他目前在部分公司中已存在之隱私專業人員。該人員可能不完全符合GDPR規定之相關條件（例如可利用之資源或獨立性之保障），倘不符合，即不能將其視為DPO或以DPO稱之。

[12] See, e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, p. 90).
「*公務機構*」及「*受公法管轄之機構*」之定義，可參照2003年11月17日歐洲議會與歐盟理事會為公部門資訊再利用制定之第2003/98/EC號指令第2條第1項及第2項。

GDPR對何謂「*公務機關或機構*」並無定義。WP29認為此一概念應由國內法決定。因此，公務機關與機構包括國家、區域及地方之機關，但此概念於國內法適用上一般也包括部分受公法管轄之其他機構[12]。於此情形下，DPO之指派為強制性。

A public task may be carried out, and public authority may be exercised[13] not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.
公共事務之執行及公權力之行使，除可能由公務機關或機構為之外，依據各會員國之國內法，也可能由受公法或私法管轄之自然人或法人行使，如大眾運輸服務、水及能源供應服務、道路基礎設施、公共廣播服務、公共住宅或法定專業人士之紀律組織等[13]。

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.
於此情形，當事人所處之情境與其資料由公務機關或機構運用之情境可能甚為相似。特別是在資料運用目的相似，且個人通常同樣對於其資料是否被運用與如何運用之選擇性甚低，或無法選擇，因此需要指派DPO給予額外保護。

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO. Such a DPO's activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).
於此情形，執行公共事務或行使公權力之私人組織雖無指派DPO之義務，WP29仍建議其指派DPO為優良作法。此種DPO之業務涵蓋所有資料運用作業，包含那些與公共事務執行及公權力行使無關（如員工資料庫管理）之作業。

2.1.2 'CORE ACTIVITIES'
核心業務

[13] Article 6(1)(e).
第6條第1項第e款。

Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor'*. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.
GDPR第37第1項第b款及c款提及「*控管者或受託運用者之核心業務*」。前言第97點明確指出，控管者之核心業務係「*與主要業務相關，與運用個資之附屬業務無關者*」。可將「核心業務」視為達成控管者或受託運用者目標之必要關鍵作業。

However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.
然而，當運用資料為控管者或受託運用者業務中所不可分割之一部分時，運用資料不應被解釋為排除在「核心業務」範圍之外。例如，醫院之核心業務為提供醫療保健。然而，醫院如不運用健康資料(如病患之健康紀錄)，即無法安全有效地提供醫療保健服務。因此，運用這些資料應視為每所醫院核心業務之一，故醫院必須指派DPO。

As another example, a private security company carries out the surveillance of a number of private shopping centres and public spaces. Surveillance is the core activity of the company, which in turn is inextricably linked to the processing of personal data. Therefore, this company must also designate a DPO.
另一個例子是，私人保全公司會對若干購物中心及公共空間進行監視。此監視工作係該公司之核心業務，亦無可避免需連結至個資運用作業。因此，此公司必須指派DPO。

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.
另一方面，有些業務是所有組織均會執行的，如支付員工薪資，或一般資訊科技支援工作。這些例子乃組織核心業務或主要經營領域所必須具備之支援功能。即使此業務係必需或必要，一般仍視為附屬功能而非核心業務。

2.1.3 'LARGE SCALE'

大規模

Article 37(1)(b) and (c) requires that the processing of personal data be carried out on a large scale in order for the designation of a DPO to be triggered. The GDPR does not define what constitutes large- scale processing, though recital 91 provides some guidance.[14]

第37條第1項第b款及c款規定，要觸發DPO之指派，個資運用需達到大規模程度。雖然前言第91點提供了一些指導[14]，但GDPR對何謂大規模運用並無定義。

Indeed, it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop for identifying in more specific and/or quantitative terms what constitutes '*large scale*' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.

的確，要訂出一個精確的運用資料數量或涉及人數之數字，且於所有情形皆可適用，是不可能的。但即使如此，也不能排除在經過一段時間後，對於某些常見的運用業務怎樣構成「*大規模*」，可發展出以較具體且/或量化的條件判斷之標準實務做法。WP29亦規劃藉由分享、公開指派DPO之相關門檻示例，以就此一發展作出貢獻。

In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

無論如何，WP29建議於判斷運用作業是否屬大規模作業時，應特別考量以下因素：

- The number of data subjects concerned - either as a specific number or as a proportion

[14] According to the recital, '*large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk*' would be included, in particular. On the other hand, the recital specifically provides that '*the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer'*. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus processing of data of a whole country or across Europe); there is a large grey zone in between these extremes. In addition, it should be borne in mind that this recital refers to data protection impact assessments. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.

依據前言，特別是「*於區域、國家或超國家層級運用大量個資為目的並可能影響大量當事人且可能造成高度風險之大規模運用作業*」將包括在內。另一方面，該前言也明確指出「*若由個別醫師、其他專業醫療保健人員或律師運用關於其病患或客戶之個資，則不應視為大規模運用個資*」。在此應留意，前言雖就運用作業之規模提供極端之範例（個別醫師辦理之運用作業，相對於全國或全歐洲之資料運用），在這些極端之間仍有相當大之灰色地帶。此外，亦應留意此前言係闡述個資保護影響評估事宜，意味部分要件可能僅適用該相關事項，而於指派DPO時並非必然同等適用。

of the relevant population
涉及之當事人數—是否達到一定數量或占相關人口之一定比例

- The volume of data and/or the range of different data items being processed
  運用之資料量及/或不同資料項目範圍
- The duration, or permanence, of the data processing activity
  資料運用作業之期間或持續性
- The geographical extent of the processing activity
  運用作業之地理涵蓋範圍

Examples of large-scale processing include:
大規模運用的例子包括：

- processing of patient data in the regular course of business by a hospital
  醫院一般作業對病患資料之運用
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
  運用個人使用城市大眾運輸系統之旅行資料（例如以票卡資料追蹤）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
  國際速食連鎖企業為統計目的，由專業之受託運用者對顧客即時地理位置資料之運用
- processing of customer data in the regular course of business by an insurance company or a bank
  保險公司或銀行一般作業上對客戶資料之運用
- processing of personal data for behavioural advertising by a search engine
  搜尋引擎為投放行為(定向)廣告對個人資料之運用
- processing of data (content, traffic, location) by telephone or internet service providers
  電信或網路服務提供者對資料（內容、流量、位置）之運用

Examples that do not constitute large-scale processing include:
不會構成大規模資料運用的例子包括：

- processing of patient data by an individual physician
  個別醫師對病患資料之運用

- processing of personal data relating to criminal convictions and offences by an individual lawyer
  個別律師對刑事前科及犯罪相關之個人資料運用

2.1.4 'REGULAR AND SYSTEMATIC MONITORING'
經常性且系統性之監控

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but the concept of '*monitoring of the behaviour of data subjects*' is mentioned in recital 24[15] and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.
經常性且系統性監控當事人之概念於GDPR中並無定義，但前言第24點已提及「*監控當事人行為*」之概念[15]，且明確包括網路上所有形式之追蹤與剖析，及為投放行為(定向)廣告之目的之行為。

However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.[16]
然而，監控之概念並不限於網路環境，線上追蹤僅應視為監控當事人行為的其中一例[16]。

WP29 interprets 'regular' as meaning one or more of the following:
WP29就「經常性」之解釋，係指以下之一項或多項情形：

- Ongoing or occurring at particular intervals for a particular period
  具持續性或於特定期間內特定間隔發生
- Recurring or repeated at fixed times
  於固定時間反覆或重複發生

---

[15] *'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.*
「*為決定該資料運用是否可受認定為監控該當事人之行為，應確認該當事人是否於網路上被追蹤，包含以個人資料運用技術對自然人進行剖析的潛在後續利用，尤其是為了作成與其有關的決策，或為分析或預測其個人偏好、行為及態度*」。

[16] Note that Recital 24 focuses on the extra-territorial application of the GDPR. In addition, there is also a difference between the wording '*monitoring of their behaviour'* (Article 3(2)(b)) and *'regular and systematic monitoring of data subjects'* (Article 37(1)(b)) which could therefore be seen as constituting a different notion.
須留意前言第24點係聚焦於GDPR之域外適用。此外，「*監控其行為*」（第3條第2項第b款）與「*對當事人經常性且系統性之監控*」文字上有所不同，故應視為不同之概念。

- Constantly or periodically taking place
  常態性或定期發生

WP29 interprets 'systematic' as meaning one or more of the following:
WP29對「系統性」之解釋，係指以下之一項或多項情形：

- Occurring according to a system
  依據一套系統設定而發生
- Pre-arranged, organised or methodical
  事先安排、有組織性或具一定方法
- Taking place as part of a general plan for data collection
  為一套整體資料蒐集計畫之一部分
- Carried out as part of a strategy
  為一項策略執行之一部分

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
可能構成對當事人經常性且系統性監控之例子包括：經營電信網路、提供電信服務、電子郵件再行銷、資料導向之行銷活動、為風險評估目的（如信用評分、保費計算、預防詐欺、洗錢偵測等）進行之剖析及評分、位置追蹤（例如以行動裝置應用程式為之）、客戶忠誠度計畫、行為(定向)廣告、透過穿戴裝置對身體狀況、體態及健康資料之監控、閉路電視、聯網裝置如智慧電表、智慧車輛、智慧家庭等。

2.1.5 SPECIAL CATEGORIES OF DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES
特種資料與刑事前科及犯罪資料

Article 37(1)(c) addresses the processing of special categories of data pursuant to Article 9, and personal data relating to criminal convictions and offences set out in in Article 10.

Although the provision uses the word 'and', there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say 'or'.
第37條第1項第c款，係規範對第9條所規定特種資料，及第10條所規定刑事前科及犯罪相關個資之運用。條文文字雖用刑事前科「及」犯罪，但並無必需同時適用該二項標準之政策理由。因此，該文字應視為刑事前科「或」犯罪。

2.2. DPO of the processor

受託運用者之DPO

Article 37 applies to both controllers[17] and processors[18] with respect to the designation of a DPO. Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).
第37條就指派DPO事宜，對控管者[17]及受託運用者[18]均適用。依哪一方符合強制指派DPO標準決定，有時僅其中一方必須指派DPO，有時兩者均應指派（如均應指派，則DPO間應相互合作）。

It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.
此處須留意，即使控管者符合強制指派DPO之標準，其受託運用者亦不必然須指派DPO，然而無論是否符合標準均指派DPO，可謂優良做法。

Examples:
範例：

- A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively

[17] The controller is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.
依據第4條第7款定義，控管者係指決定資料運用目的及方法之個人或機構。
[18] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.
依據第4條第8款定義，受託運用者係指代控管者運用資料之個人或機構。

limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

一家於單一城鎮內經營家電經銷之小型家族企業，其合作之受託運用者，係以提供網站分析服務與協助定向廣告與行銷為核心業務。此家族企業及其顧客之活動，因其顧客數量少、業務有限，不會構成「大規模」之資料運用。但該受託運用者之活動，因其有許多與此家族企業類似之客戶，其整體資料運用作業即屬大規模運用。因此該受託運用者應依第37條第1項第b款規定，指派一名DPO。同時，此家族企業則無指派DPO之義務。

- A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

  一家中型瓷磚製造商將職業健康服務外包予外部受託運用者，而該受託運用者有許多類似之客戶。因此該受託運用者應依第37條第1項第c款之大規模運用規定指派一名DPO。然而，該製造商則不必然有指派DPO之義務。

The DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

當受託運用者指派之DPO，其本身職權即屬資料控管者（如人資、資訊、物流等）時，亦應監督該受託運用者組織之活動。

2.3. Designation of a single DPO for several organisations

數個組織指派一名DPO

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects[19], the supervisory authority[20]

[19] Article 38(4): '*data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation*'.
第38條第4項：「*當事人得就依本規則運用其個資及行使其義務之所有相關事宜，與個資保護長聯繫*」。

[20] Article 39(1)(e): '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult, where appropriate, with regard to any other matter*'.
第39條第1項第e款：「*就資料運用相關事宜（包括第36條所述之事前諮商）作為與監管機關間之聯絡點，並與其於適當時就任何其他事宜進行諮商。*」

but also internally within the organisation, considering that one of the tasks of the DPO is *'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this Regulation'*.[21]
第37條第2項允許企業集團僅指派一名DPO，只要「*各據點皆易於聯繫*」該DPO。可及性之概念係指就DPO擔任當事人[19]、監管機關[20]與組織內部之聯絡點的任務而言，其中一項是「*告知與建議控管者、受託運用者及執行運用作業之員工依據本規則應盡之義務*」[21]。

In order to ensure that the DPO, whether internal or external, is accessible it is important to make sure that their contact details are available in accordance with the requirements of the GDPR.[22]
為確保DPO可被聯繫（無論內部或外部），重點在於確認其依GDPR之要求提供詳細聯絡資訊[22]。

He or she, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects[23] and cooperate[24] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.
其必須具有可有效率地與當事人溝通[23]，並與相關監管機關合作之職位[24]（必要時可由團隊協助）。此也意味著此溝通必須與監管機關及相關當事人以一種或數種語言進行。DPO之可用性（無論是與員工處於同一場所內、透過熱線電話或其他安全之通訊方式）係確保當事人可聯繫DPO之關鍵。

According to Article 37(3), a single DPO may be designated for several public authorities or

[21] Article 39(1)(a).
第39條第1項第a款。
[22] See also Section 2.6 below.
另參照第2.6節以下說明。
[23] Article 12(1): *'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'*
第12條第1項：「*控管者應採取適當措施，以簡潔、透明、易懂且便於取得之形式，使用清晰、平易的語言文字，提供當事人第13條及第14條所述之所有資訊，並與當事人依第15條至第22條及第34條規定就關於資料運用進行所有溝通，尤其是任何明確指涉兒童之資訊。*」
[24] Article 39(1)(d) *: 'to cooperate with the supervisory authority'*
第39條第1項第d款：「*與監管機關合作*」。

bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.
依據第37條第3項，數個公務機關或機構於衡量其組織架構及規模後，可指派單一DPO。前述有關資源及溝通之考量在此亦適用。因DPO掌理許多不同之任務，控管者或受託運用者必須確保此單一DPO即使為數個公務機關或機構所指派，仍可有效率地執行任務（必要時可由團隊協助）。

2.4. Accessibility and localisation of the DPO
DPO之可及性及在地化

According to Section 4 of the GDPR, the accessibility of the DPO should be effective.
依據GDPR第4節規定，DPO應具備有效之可及性。

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union.
為確保DPO之可及性，WP29建議，無論控管者或受託運用者是否於歐盟境內設立，DPO均應設置於歐盟境內。

However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union[25], a DPO may be able to carry out his or her activities more effectively if located outside the EU.
然而，不排除於某些情形下，控管者或受託運用者於歐盟境內未設置據點時[25]，DPO如設於歐盟境外，可能可更有效執行其業務。

2.5. Expertise and skills of the DPO
DPO之專業及技能

Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'. Recital 97 provides that the necessary level of expert

[25] See Article 3 of the GDPR on the territorial scope.
詳參GDPR第3條關於領域範圍之規定。

knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.
第37條第5項規定DPO「*應以其專業能力，尤以其對資料保護法規與實務之專業知識，及確實達成第39條所述任務之能力，為指派基礎*」。前言第97點則敘明，必要之專業知識程度應視所執行之資料運用作業，及所運用之個人資料所需之保護措施而定。

- Level of expertise
  專業程度

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.
對專業程度之要求並無嚴格定義，但必須與組織所運用資料之敏感性、複雜度及資料量相應。舉例而言，當資料運用作業特別複雜，或涉及大量敏感資料時，DPO可能需要更高之專業程度及支援。該組織係系統性將個資傳輸至歐盟境外或偶爾為之，對DPO專業程度之要求亦有所不同。因此，DPO之選任應依組織內產生之資料保護相關問題適當考量並謹慎為之。

- Professional qualities
  專業能力

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.
儘管第37條第5項並未明確規定指派DPO時應考量之專業能力，但相關要件是DPO必須具備國內及歐盟資料保護法規與實務專業，及對GDPR之深入了解。監管機關如可推動適當的、定期的DPO訓練，亦有所幫助。

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

對產業及控管者之組織的知識是有助益的。DPO亦應對控管者之資料運用作業、資訊系統、資料安全及資料保護需求有深入了解。

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.
如係公務機關或機構，DPO則亦應對該組織之行政規章及程序有充分的知識。

- Ability to fulfil its tasks
  達成任務之能力

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing[26], data subjects' rights[27], data protection by design and by default[28], records of processing activities[29], security of processing[30], and notification and communication of data breaches.[31]
DPO達成其所肩負任務之能力，應解釋為同時包含其個人素質、知識，及其於組織內之職位。個人素質，應包括如誠信及高度之職業倫理；DPO之首要考量應係促成GDPR之法遵。DPO於培養組織內資料保護文化扮演關鍵角色，且有助於GDPR中重要元素如資料運用原則[26]、當事人權利[27]、以資料保護為系統設計目的及預設選項[28]、運用作業紀錄[29]、運用作業安全[30]，及資料侵害通報及溝通[31]等之執行。

- DPO on the basis of a service contract
  以服務契約為基礎之DPO

The function of the DPO can also be exercised on the basis of a service contract concluded

[26] Chapter II.
第二章。
[27] Chapter III.
第三章。
[28] Article 25.
第25條。
[29] Article 30.
第30條。
[30] Article 32.
第32條。
[31] Articles 33 and 34.
第33及第34條。

with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that each member of the organisation exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.
DPO之功能亦可由控管者/受託運用者與組織以外之個人或組織簽署服務契約來執行。如係後者（與組織簽署契約）之情形，則重要的是此簽約對象之組織中執行DPO功能之成員均符合GDPR第4節規定中所有應適用之要求（例如成員中無人有利益衝突）。同樣重要的是，每一位此種成員皆受GDPR條文之保護（例如不因執行DPO業務而遭不當終止服務契約，及組織中執行DPO業務之個人不因此而遭不當解僱等）。同時，亦可以團隊方式結合數人之技能及特長，得以更有效率地服務其客戶。

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.
為求法律上之明確性及良好之組織，並防止團隊成員之利益衝突，建議DPO團隊內應有明確分工，並就每個客戶指派一人為主要聯絡人及「負責」人。在服務契約中敘明前述各事項乃常見且實用。

2.6. Publication and communication of the DPO's contact details
DPO詳細聯絡資訊之公布及傳達

Article 37(7) of the GDPR requires the controller or the processor:
GDPR第37條第7項要求控管者或受託運用者應：

- to publish the contact details of the DPO and
  公布DPO之詳細聯絡資訊，並
- to communicate the contact details of the DPO to the relevant supervisory authorities.
  將DPO之詳細聯絡資訊提供予相關監管機關。

The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) and the supervisory authorities can easily and directly contact the DPO

without having to contact another part of the organisation. Confidentiality is equally important: for example, employees may be reluctant to complain to the DPO if the confidentiality of their communications is not guaranteed.
此要求之目的係為確保（無論組織內外之）當事人及監管機關可以容易地、直接地與DPO聯繫，而無需聯繫組織之其他部門。保密亦具同等重要性，舉例而言，如員工與DPO間之通訊保密未受保障，則其可能不願向DPO提出申訴。

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)).
依據歐盟及會員國法律，DPO就其任務之執行情形應予保密（第38條第5項）。

The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.
DPO之詳細聯絡資訊，應包含可使當事人及監管機關容易與DPO取得聯繫之資訊（郵寄地址、專線電話及/或專用電郵信箱）。為與大眾溝通，於適當情況，亦可提供其他通訊方式，例如專用熱線電話或於組織網站上與DPO聯繫之專用連絡表單。

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.[32]
第37條第7項並非要求所公布之聯絡資訊應包含DPO之姓名。雖然公布姓名或為優良作法，但在特定情形下公布DPO姓名是否必要或有助益，應由控管者或受託運用者與DPO決定[32]。

However, communication of the name of the DPO to the supervisory authority is essential in order for the DPO to serve as contact point between the organisation and the supervisory authority (Article 39(1)(e).
然而，將DPO之姓名提供予監管機關，係DPO作為組織與監管機關間聯絡點之重要事

[32] It is notable that Article 33(3)(b), which describes information that must be provided to the supervisory authority and to the data subjects in case of a personal data breach, unlike Article 37(7), specifically also requires the name (and not only the contact details) of the DPO to be communicated.
應留意第33條第3項第b款闡述了如發生個資外洩事件時必須提供予監管機關及當事人之資訊，且與第37條第7項規定不同的是，該款明確要求提供DPO之姓名（而非僅聯絡資訊）。

項（第39條第1項第e款）。

As a matter of good practice, the WP29 also recommends that an organisation informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.
WP29亦建議，組織將其DPO之姓名及聯絡資訊告知員工，係為優良做法。舉例而言，DPO之姓名及聯絡資訊可由組織內網、內部電話表及組織圖等方式對內公布。

3 Position of the DPO
DPO之職位

3.1. Involvement of the DPO in all issues relating to the protection of personal data
DPO對所有個資保護相關事宜之參與

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is *'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'.*
GDPR第38條規定，控管者及受託運用者應確保DPO「*適切且即時地參與所有個資保護相關事宜*」。

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.[33] Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.
DPO或其團隊儘量於所有資料保護相關事宜之前期即參與其中，具關鍵重要性。就個資保護影響評估而言，GDPR對DPO於前期之參與已有明文規定，並明確指出控管者辦理該影響評估時，應尋求DPO之建議[33]。確保DPO於一開始即知情且受到諮詢，將可促進對GDPR之法遵、推動以隱私保護為系統設計目的之方法，故應係組織內部治理之標

[33] Article 35(2).
第35條第2項。

準程序。此外，組織內部將DPO視為可共同討論之夥伴，並將其納入組織內資料運用作業相關之工作小組，亦至關重要。

Consequently, the organisation should ensure, for example, that:
因此，舉例而言，組織應確保以下事項：

- The DPO is invited to participate regularly in meetings of senior and middle management.
  DPO應受邀定期參與管理高層及中階主管之會議。
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
  進行之決策可能對資料保護產生影響時，建議DPO應在場。所有相關資訊均應即時傳遞予DPO，以利其提供充足之建議。
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
  DPO之意見必須予適當尊重。如出現意見不同情形，WP29建議記錄未遵循DPO建議之理由，為優良做法。
- The DPO must be promptly consulted once a data breach or another incident has occurred.
  如發生資料侵害或其他事故，應即時諮詢DPO。

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.
控管者或受託運用者可於適當時機研擬資料保護指引或計畫，規範何時應諮詢DPO。

3.2. Necessary resources
必要資源

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.* The following items, in particular, are to be considered:
GDPR第38條第2項要求組織應以「*提供執行〔其〕任務、存取個資及個資運用作業，*

及維持其專業知識之必要資源」支援DPO。特別應考量以下項目：

- Active support of the DPO's function by senior management (such as at board level).
  於管理高層（如董事會層級）積極支持DPO之功能。
- Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
  給予DPO充足時間完成職責。尤其是如果DPO係由組織內部人員兼任，或外部DPO於執行資料保護業務外亦具其他職責時，特別重要。否則，各項工作優先順序之衝突可能造成DPO之職責遭到忽略。有充足時間來執行DPO之任務至關重要。如DPO係兼任，則明定一定比例之時間執行DPO工作係優良做法。決定執行相關功能所需之時間及DPO職責適當之優先層級，以及由DPO（或由組織）研擬工作計畫，亦係優良做法。
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
  適當之財務資源、基礎設施（場所、設備、器材）及人員之充足支援。
- Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
  就DPO之指派正式傳達所有員工，以確保組織內部知悉其存在及功能。
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
  DPO應可取得其他必需之服務，如人資、法務、資訊、資安等，使其可自該等服務管道獲得必要之支援、資源投入及資訊。
- Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional

development, such as participation in privacy fora, workshops, etc.
持續之訓練。DPO必須有機會持續瞭解資料保護領域之新發展。訓練之目標應係持續增進DPO之專業程度，且應鼓勵DPO參與資料保護相關訓練課程及其他形式之專業發展，如隱私論壇、工作坊等。

- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.
視組織大小及結構，設置DPO團隊（即DPO本人及其成員）或有其必要。在此情形下，團隊內部之架構及其成員之任務及職責應明確訂定。同理，當DPO之功能係由外部服務提供者執行時，若干個人組成之團隊可指派一名對客戶的主要聯絡人，有效地以團隊方式實際執行DPO之任務。

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.
一般而言，運用作業越複雜及/或敏感，必須給予DPO之資源就越多。資料保護之功能須有效，且具備與所辦理之資料運用作業相對應之充分資源。

3.3. Instructions and '*performing their duties and tasks in an independent manner*'
指示及「*獨立執行其職責及任務*」

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO '*does not receive any instructions regarding the exercise of [his or her] tasks.*' Recital 97 adds that DPOs, '*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*'.
第38條第3項確立了若干確保DPO可於組織中執行任務時具充足自主性之基本保障事項。特別是要求控管者/受託運用者應確保DPO「*免於接受任何有關執行（其）任務之指示*」。前言第97點亦補充說明DPO「*無論是否受僱於控管者，都應該能以獨立方式執行其職責和任務*」。

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.

此意味DPO於執行第39條規定之任務時，DPO不得接受應如何處理事務之指示，例如應達成何種結果、如何調查申訴案或是否應諮詢監管機關等。此外，DPO不得就資料保護法規相關議題，接受應採特定見解之指示，例如採特定之法規解釋等。

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

然而，DPO之自主性，不代表其具有超越第39條所規定任務範圍以外之決策權。

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.[34] If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO '*shall directly report to the highest management level of the controller or the processor'*. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.

控管者或受託運用者仍肩負遵守資料保護法規之責，且應能證明其合規[34]。如控管者或受託運用者之決策與GDPR及DPO之建議不符，應賦予DPO向最高管理階層，及此決策之決策者，釐清其不同意見之可能性。就此部分，第38條第3項規定，DPO「*應直接向控管者或受託運用者之最高管理階層報告*」。此直接報告可確保高層管理者（例如董事會）知悉DPO依其告知及向控管者或受託運用者提供建議之職務，所提出之意見及建議事項。另一種直接報告之範例為撰擬DPO業務年度報告，提交予最高管理階層。

3.4. Dismissal or penalty for performing DPO tasks

DPO因執行任務而遭解僱或處罰

Article 38(3) requires that DPOs should *'not be dismissed or penalised by the controller or*

[34] Article 5(2).
第5條第2項。

the processor for performing [their] tasks'.
第38條第3項規定DPO「*不應因執行〔其〕任務而遭控管者或受託運用者解僱或處罰*」。

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.
此要求強化了DPO之自主性，且有助於確保DPO獨立作業，並就執行其資料保護業務享有充足之保護。

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.
因執行其DPO之職責而導致其受處罰，僅於GDPR中受禁止。例如，DPO可能認為某項特殊的運用可能導致高風險，而建議控管者或受託運用者進行個資保護影響評估，但控管者或受託運用者並不同意DPO之評估。在此情形下，DPO不應因提出此項建議而遭解僱。

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.
處罰可能採取不同之形式，也可能是直接或間接的。可能包括例如不予升職或延遲升職、阻擋職涯發展、不提供其他員工可得之福利等。不必然需實際處罰，只要處罰DPO是與其業務有關，僅是威脅即足以構成。

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).
DPO仍可因執行其任務以外之正當理由（例如竊盜、生理、心理、性騷擾或其他類似之嚴重不當行為等）被解僱，此係一般之管理原則，與適用國內契約或勞工、刑事法律之其他員工或契約人員相同。

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

在此應留意，GDPR並未明定如何與何時可解僱或以他人取代DPO。然而，DPO之合約越穩定，不受不當解僱之保障越高，其將越有可能獨立執行職務。因此，WP29樂見各組織朝此方向努力。

3.5. Conflict of interests

利益衝突

Article 38(6) allows DPOs to '*fulfil other tasks and duties'*. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests'*.

第38條第6項容許DPO「*執行其他任務及職責*」。但該項亦要求該組織確保「*此任務或職責不會造成利益衝突*」。

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

無利益衝突之概念與獨立執行職務密切相關。雖允許DPO可有其他功能，但僅在不造成利益衝突之前提下，方可賦予DPO其他任務及職責。確切來說，此意味DPO不得擔任組織中決定個資運用目的及方式之職位。因各組織之組織結構不同，此部分必須依個案考量。

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

一般而言，組織內利益衝突之職位可能包含管理高層（如執行長、營運長、財務長、醫療長、行銷部主管、人資部主管、技術長等），但如組織結構中較低階之職位會決定個資運用之目的及方式，則亦可能包含該職位。此外，例如外部DPO代表控管者或受託運用者就資料保護爭議至法院出庭時，亦可能發生利益衝突。

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:
依個別組織之業務、規模及結構不同，以下可為控管者或受託運用者之優良做法：

- to identify the positions which would be incompatible with the function of DPO
  確認與DPO功能無法相容之職位
- to draw up internal rules to this effect in order to avoid conflicts of interests
  就此擬定避免利益衝突之內規
- to include a more general explanation about conflicts of interests
  包含對利益衝突之一般性解釋文字
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
  聲明其DPO就其擔任DPO之功能並無利益衝突，以提高對此要求之意識
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally
  將相關安全機制納入組織內規，並確保DPO之職缺公告或服務契約足夠精確與詳盡，以避免利益衝突。此處亦應留意利益衝突可能依DPO係內部或外部雇用人員，而有不同之形式。

4 Tasks of the DPO
DPO之任務

4.1. Monitoring compliance with the GDPR
監督對GDPR之法遵事宜

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO '*should assist the controller or the processor*

to monitor internal compliance with this Regulation'.
第39條第1項第b款賦予DPO任務之一係監督對GDPR之法遵事宜。前言第97點進一步說明DPO「*應協助控管者或受託運用者監督組織內部對本規則之遵循事宜*」。

As part of these duties to monitor compliance, DPOs may, in particular:
具體而言，DPO得於監督法遵之職責範圍內：

- collect information to identify processing activities
  蒐集資訊以確認運用作業
- analyse and check the compliance of processing activities
  分析並檢視運用作業之法遵
- inform, advise and issue recommendations to the controller or the processor
  通知、勸告及提出建議予控管者或受託運用者

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.
監督法遵並不表示發生未遵法事件時，應由DPO本人負責。GDPR明確規定，應「*採取適當的技術性和組織性措施，確保並得以證明依本規則執行運用*」者，為控管者而非DPO（第24條第1項）。資料保護法遵是資料控管者之公司責任，而非DPO之責任。

4.2. Role of the DPO in a data protection impact assessment
DPO於個資保護影響評估中之角色

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice'* of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35*'.
依據第35條第1項規定，於必要時辦理個資保護影響評估（DPIA）係控管者而非DPO之任務。然而，DPO於協助控管者上，可扮演非常重要且實用之角色。第35條第2項依

循以資料保護為系統設計目的之原則，明確要求控管者於辦理DPIA時「*應徵詢DPO之意見*」。而第39條第1項第c款，則賦予DPO「*應依第35條規定就〔DPIA〕提供建議並監督其執行*」之職責。

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others [35]:
WP29建議控管者應至少就以下事宜徵詢DPO之建議[35]：

- whether or not to carry out a DPIA
  是否辦理DPIA
- what methodology to follow when carrying out a DPIA
  辦理DPIA時應採取之方法
- whether to carry out the DPIA in-house or whether to outsource it
  DPIA應由組織內部辦理或委外辦理
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
  應採取何種安全措施（包含技術性及組織性措施）以降低當事人權利及利益之風險
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR
  個資保護影響評估是否依正確方式辦理，及其結論（是否於運用前辦理及採取何種安全措施）是否遵循GDPR規範

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account[36].

---

[35] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have '*at least'* the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail.
第39條第1項提及DPO之任務，並敘明DPO「*至少*」應有以下任務。因此，並未禁止控管者分派第39條第1項明文規定範圍以外之其他任務予DPO或將這些任務作更明確、詳細之說明。

[36] Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure* ***and to be able to demonstrate*** *that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'.
第24條第1項規定「*考量運用之性質、範圍、背景和目的，以及不同可能性與嚴重性對自然人的權利及自由造成之風險，控管者應採取適當的技術性和組織性措施，確保****並得以證明****依本規則執行運用。必要時應檢視並*

如控管者不同意DPO之諮詢意見，DPIA文件中應以書面明確記載未採納該意見之正當理由[36]。

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.
WP29進一步建議控管者，於DPO之合約及提供予員工、管理階層（及其他有關之利害關係人）之資訊等，明確指出DPO之確切任務及涵蓋範圍，特別是辦理DPIA之相關事項。

4.3. Cooperating with the supervisory authority and acting as a contact point
與監管機關合作並作為聯絡點

According to Article 39(1)(d) and (e), the DPO should '*cooperate with the supervisory authority*' and '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter'*.
依據第39條第1項第d款及e款，DPO應「*與監管機關合作*」並「*就資料運用相關事宜，包含第36條規定之事前諮詢，作為對監管機關之聯絡點，並於適當時就任何其他事宜向監管機關諮詢*」。

These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.
這些任務涉及本指引導言中提及DPO作為「促進者」之角色。DPO係以作為聯絡點方式使監管機關便於取得文件及資訊，以執行第57條所述之任務，並行使第58條所述之

更新這些措施」。

調查、糾正、授權、建議等權力。如前所述，DPO就其任務執行事宜，依據歐盟或會員國法規負有保密之責（第38條第5項）。然而，此保密義務並非禁止DPO聯繫監管機關並徵詢其意見。第39條第1項第e款規定，DPO亦可於適當時就任何其他事宜徵詢監管機關之意見。

4.4. Risk-based approach

以風險為基礎之方法

Article 39(2) requires that the DPO '*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*'.

第39條第2項要求DPO「*基於運用之性質、範圍、脈絡及目的，考量運用作業的相關風險*」。

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

此條文重述了一項與DPO日常業務許多方面皆相關之一般常識性原則。本質上，此條文要求DPO應將業務排列優先順序，努力聚焦在資料保護風險較高之議題。此非謂DPO即應忽略對風險相對較低資料運用作業之法遵監督，而係表示其主要應專注於風險較高之領域。

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

此種有選擇性的且務實的方法，應可幫助DPO就辦理DPIA應採取之方式、何種範圍應辦理內部或外部資料保護稽核、應提供予負責資料運用作業員工或管理階層何種內部訓練，及應投入其較多時間及資源於何種運用作業等事宜，向控管者提供諮詢意見。

4.5. Role of the DPO in record-keeping

DPO於紀錄保存之角色

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to '*maintain a record of processing operations under its responsibility*' or *'maintain a record of all categories of processing activities carried out on behalf of a controller'.*
依第30條第1項及第2項規定，應「*維護其所負責之運用作業紀錄*」或「*維護其代控管者辦理之所有運用作業類別紀錄*」者，係控管者或受託運用者，而非DPO。

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[37]
實務上，DPO常會依據組織內負責運用個資部門提供之資訊，建立、保留一份運用作業及登記清冊。此作法於許多現行國內法及歐盟機關、機構所適用之資料保護規章中，已訂有明文[37]。

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
第39條第1項所列之工作項目，乃對DPO之最低限度要求。因此，控管者或受託運用者就其所負責之運用作業，指派DPO維護紀錄，亦無不可。該等紀錄應視為DPO執行其監督法遵事宜，及向控管者或受託運用者提供資訊及建議等任務之工具之一。

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.
無論如何，依第30條規定應保留之紀錄，亦應視為使控管者及監管機關，得應要求檢視組織所辦理所有個資運用作業之工具。因此，該紀錄係法遵之先決條件，與有效之課責性措施。

[37] Article 24(1)(d), Regulation (EC) 45/2001.
歐盟第45/2001號規則第24條第1項第d款。

5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW
附錄—DPO指引：你應該要知道的事

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the General Data Protection Regulation (*GDPR) to appoint a DPO.*
此附錄之目的，係以簡化、易讀之形式，解答各組織依據一般資料保護規則（GDPR）所定之新要件指派DPO事宜之重要問題。

Designation of the DPO
DPO之指派

1 Which organisations must appoint a DPO?
什麼組織必須指派DPO？

The designation of a DPO is an obligation:
於下列情形下，有義務指派DPO：

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
  運用作業係由公務機關或機構辦理（無論運用之資料為何）
- if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
  控管者或受託運用者之核心業務包含對當事人進行經常性、系統性大規模監控之運用作業
- if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences
  控管者或受託運用者之核心業務，包含大規模運用特種資料或與刑事前科及犯罪相關之個人資料

Note that Union or Member State law may require the designation of DPOs in other situations as well. Finally, even if the designation of a DPO is not mandatory, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts. When an organisation

designates a DPO on a voluntary basis, the same requirements will apply to his or her designation, position and tasks as if the designation had been mandatory.
此處須留意，歐盟或會員國法規可能要求於其他情形下亦須指派DPO。最後，即使於非強制指派DPO之情形下，組織有時會發現自願性指派DPO有其益處。第29條個資保護工作小組（WP29）亦鼓勵此自願性之努力。如組織自願指派DPO，該DPO之指派、職位及任務即適用強制指派之標準。

Source: Article 37(1) of the GDPR
資料來源：GDPR第37條第1項

2 What does 'core activities' mean?
何謂「核心業務」？

'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.
「核心業務」可視為達成控管者或受託運用者目標之關鍵性作業。此亦包含控管者或受託運用者以運用資料為其不可分割的一部分之所有業務。例如，運用病人病歷等醫療資料應視為任何一所醫院之核心業務之一，故醫院亦必須指派DPO。

On the other hand, all organisations carry out certain supporting activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.
另一方面，某些支援性業務是所有組織均會辦理的，如支付員工薪資，或進行一般性之資訊科技支援工作。此係組織之核心業務或主要經營領域所必須具備之支援功能。即使該業務是必要的或不可缺的，一般仍視為附屬功能而非核心業務。

Source: Article 37(1)(b) and (c) of the GDPR
資料來源：GDPR第37條第1項第b款及c款

3 What does 'large scale' mean?
何謂「大規模」？

The GDPR does not define what constitutes large-scale processing. The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
GDPR對何謂大規模運用並無定義。WP29建議於判斷運用作業是否屬大規模時，應特別考量以下因素：

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
  涉及之當事人數—是否達到一定數量或占相關人口之一定比例
- the volume of data and/or the range of different data items being processed
  運用之資料量及/或不同資料項目範圍
- the duration, or permanence, of the data processing activity
  資料運用作業之期間或持續性
- the geographical extent of the processing activity
  運用作業之地理涵蓋範圍

Examples of large scale processing include:
大規模運用的例子包括：

- processing of patient data in the regular course of business by a hospital
  醫院一般作業對病患資料之運用
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
  運用個人使用城市大眾運輸系統之旅行資料（例如以票卡資料追蹤）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
  國際速食連鎖企業為統計目的，由專業之受託運用者對顧客即時地理位置資料之運用
- processing of customer data in the regular course of business by an insurance company or a bank
  保險公司或銀行一般作業上對客戶資料之運用
- processing of personal data for behavioural advertising by a search engine
  搜尋引擎為投放行為(定向)廣告對個人資料之運用

- processing of data (content, traffic, location) by telephone or internet service providers
  電信或網路服務提供者對資料（內容、流量、位置）之運用

Examples that do not constitute large-scale processing include:
不會構成大規模資料運用的例子包括：

- processing of patient data by an individual physician
  個別醫師對病患資料之運用
- processing of personal data relating to criminal convictions and offences by an individual lawyer
  個別律師對刑事前科及犯罪相關之個人資料運用

Source: Article 37(1)(b) and (c) of the GDPR
資料來源：GDPR第37條第1項第b款及c款

4 What does 'regular and systematic monitoring' mean?
何謂「經常性且系統性監控」？

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.
經常性且系統性監控當事人之概念於GDPR中並無定義，但明顯包含所有形式，包括為投放行為定向廣告所做的網路追蹤與剖析。然而，監控之概念並不限於網路環境。

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
可能構成對當事人經常性且系統性監控之例子包括：經營電信網路、提供電信服務、電子郵件再行銷、資料導向之行銷活動、為風險評估目的（如信用評分、保費計算、預防詐欺、洗錢偵測等）進行之剖析及評分、位置追蹤（例如以行動裝置應用程式為

之）、客戶忠誠度計畫、行為（定向）廣告、透過穿戴裝置對身體狀況、體態及健康資料之監控、閉路電視、聯網裝置如智慧電表、智慧車輛、智慧家庭等。

WP29 interprets 'regular' as meaning one or more of the following:
WP29就「經常性」之解釋，係指以下之一項或多項情形：

- ongoing or occurring at particular intervals for a particular period
  具持續性或於特定期間內特定間隔發生
- recurring or repeated at fixed times
  於固定時間反覆或重複發生
- constantly or periodically taking place
  常態性或定期發生

WP29 interprets 'systematic' as meaning one or more of the following:
WP29對「系統性」之解釋，係指以下之一項或多項情形：

- occurring according to a system
  依據一套系統設定而發生
- pre-arranged, organised or methodical
  事先安排、有組織性或具一定方法
- taking place as part of a general plan for data collection
  為一套整體資料蒐集計畫之一部分
- carried out as part of a strategy
  為一項策略執行之一部分

Source: Article 37(1)(b) of the GDPR
資料來源：GDPR第37條第1項第b款

5 Can organisations appoint a DPO jointly? If so, under what conditions?
多個組織可否共同指派一名DPO？若可，條件為何？

Yes. A group of undertakings may designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation. In order to ensure that the DPO is accessible, whether internal or external, it is important to make sure that their contact details are available. The DPO, with

the help of a team if necessary, must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.
可以。企業集團可指派單一DPO，只要此DPO能「*便於各據點聯繫*」。可及性之概念係指DPO擔任當事人、監管機關及組織內部聯絡點之任務。為確保DPO之可及性（無論內部或外部），重要的是應確認DPO之聯絡資訊為正確可用的。其必須具有可有效率地與當事人溝通，並與相關監管機關合作之職位（必要時可由團隊協助）。此也意味著該溝通必須與監管機關及相關當事人以一種或數種語言進行。DPO之可用性（無論是與員工處於同一場所內、透過熱線電話或其他安全之通訊方式聯繫）係確保當事人可聯繫DPO之關鍵。

A single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.
多個公務機關或機構於衡量其組織架構及規模後，可指派單一DPO。前述有關資源及溝通之考量在此亦適用。因DPO掌理許多不同之任務，控管者或受託運用者必須確保此單一DPO即使被多個公家機關或機構指派，仍可有效率地執行此任務（必要時可由團隊協助）。

Source: Article 37(2) and (3) of the GDPR
資料來源：GDPR第37條第2項及第3項

6 Where should the DPO be located?
DPO應設置於何處？

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union. However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.
為確保DPO之可及性，WP29建議，無論控管者或受託運用者是否於歐盟境內設立，

DPO均應設置於歐盟境內。然而，不排除於某些情形下，控管者或受託運用者於歐盟境內未設置據點時，DPO如設於歐盟境外，可能可更有效執行其業務。

7 Is it possible to appoint an external DPO?
是否可指派組織外部之DPO？

Yes. The DPO may be a staff member of the controller or the processor (internal DPO) or fulfil the tasks on the basis of a service contract. This means that the DPO can be external, and in this case, his/her function can be exercised based on a service contract concluded with an individual or an organisation.
可以。DPO可以是控管者或受託運用者之員工（內部DPO）或依服務契約履行任務。此表示DPO可由外部人員擔任，於此情形下，得基於與個人或組織簽訂之服務契約實踐其功能。

When the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable requirements of the GDPR.
當DPO之功能係由外部服務提供者執行時，於指定之主要聯絡與「負責」該客戶之人主責下，受僱於該服務提供者的一組人，得以團隊方式有效執行DPO之任務。在此情形下，此執行DPO之外部組織中每一成員均應符合GDPR對DPO適用之所有資格要求。

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, the Guidelines recommend to have, in the service contract, a clear allocation of tasks within the external DPO team and to assign a single individual as a lead contact and person 'in charge' of the client.
為求法律上之明確性及良好之組織，並防止團隊成員之利益衝突，此指引建議在服務契約中敘明外部DPO團隊之分工，並指派一人為主要聯絡人及「負責」人。

Source: Article 37(6) of the GDPR
資料來源：GDPR第37條第6項

8 What are the professional qualities that the DPO should have?
DPO應具備何專業？

The DPO shall be designated on the basis of professional qualities and, in particular, expert

knowledge of data protection law and practices and the ability to fulfil his or her tasks.
DPO應以其專業能力，特別是對資料保護法規與實務之專業知識，及達成任務之能力，為指派之基礎。

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.
必要之專業知識程度應視所執行之資料運用作業，及所運用之資料所需之保護措施而定。舉例而言，當資料運用作業特別複雜，或涉及大量敏感資料時，DPO可能需要更高之專業程度及支援。

Relevant skills and expertise include:
相關之技能及專業包括：

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
  對國內及歐洲資料保護法規及實務之專業，包括對GDPR之深入了解
- understanding of the processing operations carried out
  對組織所辦理之資料運用作業之瞭解
- understanding of information technologies and data security
  對資訊科技及資料安全之瞭解
- knowledge of the business sector and the organization
  對產業及組織之知識
- ability to promote a data protection culture within the organization
  於組織內推動資料保護文化之能力

Source: Article 37(5) of the GDPR
資料來源：GDPR第37條第5項。

Position of the DPO DPO之職位

9 What resources should be provided to the DPO by the controller or the processor? 控管者或受託運用者應提供DPO什麼資源？

The DPO must have the resources necessary to be able to carry out his or her tasks.
DPO必須擁有使其可執行任務之必要資源。

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:
視運用作業之性質及組織業務與規模之不同，以下資源應提供予DPO：

- active support of the DPO's function by senior management
  管理高層對DPO功能之積極支持
- sufficient time for DPOs to fulfil their tasks
  讓DPO完成其任務之充足時間
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
  於適當情形下，提供充足之財務資源、基礎設施（場所、設備、器材）及人員支援
- official communication of the designation of the DPO to all staff
  就DPO之指派正式傳達予所有員工
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
  DPO應可自組織內取得其他服務，使其可從這些服務得到必要之支援、資源投入及資訊
- continuous training
  持續之訓練

Source: Article 38(2) of the GDPR
資料來源：GDPR第38條第2項

10 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner? What does 'conflict of interests' mean?
使DPO可獨立執行其任務之安全措施為何？何謂「利益衝突」？

Several safeguards exist in order to enable the DPO to act in an independent manner:
確保DPO獨立作業之安全措施如下：

- no instructions by the controllers or the processors regarding the exercise of the DPO's

tasks
控管者或受託運用者不就DPO執行任務下達任何指示

- no dismissal or penalty by the controller for the performance of the DPO's tasks
  DPO不會因執行其任務而遭控管者解僱或處罰
- no conflict of interest with possible other tasks and duties
  不會與其他可能之任務或職責產生利益衝突

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.
DPO之其他任務或職責不得造成利益衝突。此意味首先DPO不得擔任組織中可決定個資運用作業目的及方式之職位。因各組織之組織結構不同，此部分必須依個案考量。

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.
一般而言，組織內利益衝突之職位可能包含管理高層（如執行長、營運長、財務長、醫療長、行銷部主管、人資部主管、技術長等），但如組織結構中較低階之職位會決定個資運用之目的及方式，則亦可能包含該職位。此外，例如外部DPO代表控管者或受託運用者就資料保護爭議至法院出庭時，亦可能發生利益衝突。

Source: Article 38(3) and 38(6) of the GDPR
資料來源：GDPR第38條第3項及第38條第6項

Tasks of the DPO
DPO之任務

---

11 What does 'monitoring compliance' mean?
何謂「監督法遵事宜」？

As part of these duties to monitor compliance, DPOs may, in particular:
具體而言，DPO得於監督法遵之職責範圍內：

- collect information to identify processing activities
  蒐集資訊以確認運用作業
- analyse and check the compliance of processing activities
  分析並檢視運用作業之法遵
- inform, advise and issue recommendations to the controller or the processor
  通知、勸告及提出建議予控管者或受託運用者

Source: Article 39(1)(b) of the GDPR
資料來源：GDPR第39條第1項第b款

12 Is the DPO personally responsible for non-compliance with data protection requirements?
DPO本人是否需為未遵循資料保護之要求負責？

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Data protection compliance is the responsibility of the controller or the processor.
不需要。DPO本人無須為未遵循資料保護之要求負責。應確保並得以證明依本規則執行運用者為控管者或受託運用者。資料保護法遵係控管者或受託運用者之責任。

13 What is the role of the DPO with respect to data protection impact assessments and records of processing activities?
DPO於個資保護影響評估及運用作業紀錄保存之角色為何？

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:
在個資保護影響評估方面，控管者或受託運用者應至少就以下事宜徵詢DPO之意見：

- whether or not to carry out a DPIA
  是否辦理DPIA
- what methodology to follow when carrying out a DPIA
  辦理DPIA應採取之方法

- whether to carry out the DPIA in-house or whether to outsource it
  DPIA應由組織內部辦理或委外辦理
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
  應採取何種安全措施（包含技術性及組織性措施）以降低當事人權利及利益之風險
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements
  個資保護影響評估是否依正確方式辦理，及其結論（是否於運用前辦理及採取何種安全措施）是否遵循資料保護要求

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
在運用作業紀錄方面，係控管者或受託運用者應保留運用作業紀錄，而非DPO。然而，並未禁止控管者或受託運用者就其所負責之運用作業，指派DPO維護紀錄。該紀錄應視為使DPO得以執行其監督法遵、向控管者或受託運用者提供資訊及建議等任務的工具之一。

Source: Article 39(1)(c) and Article 30 of the GDPR
資料來源：GDPR第39條第1項第c款及第30條

Done in Brussels, on 13 December 2016
2016年12月13日於布魯塞爾完成

For the Working Party 工作小組
The Chairwoman 主席
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

2017年4月5日最新修訂並通過

For the Working Party 工作小組

The Chairwoman 主席

Isabelle FALQUE-PIERROTIN

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

17/EN
WP260 rev.01

Article 29 Working Party
第29條個資保護工作小組
Guidelines on transparency under Regulation 2016/679
關於第2016/679號規則(GDPR)中的透明化之指引

Adopted on 29 November 2017

As last Revised and Adopted on 11 April 2018

2017年11月29日通過

2018年4月11日最後修訂並通過

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item type=1358&tpa id=6936

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

*註釋：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Table of Content 目錄

Introduction

導言

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation[1] (the "**GDPR**"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights[2]. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680[3], these guidelines also apply to the interpretation of that principle.[4] These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

   本指引係29條工作小組（WP29）依據一般資料保護規則（**GDPR**）[1]中就運用個人資料新設的透明化義務提供實務指導和解釋性協助。透明化是GDPR下的總體義務，且適用於三項主要領域：（1）向當事人提供公正運用之相關資訊；（2）資料控管者如何與當事人就其在GDPR下之權利進行溝通；以及（3）資料控管者如何使當事人便於行使其權利[2]。為遵循(EU)第2016/680號指令[3]下關於資料運用之透明化要求，本指引亦適用於該原

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
2016年4月27日歐洲議會與歐盟理事會在個人資料運用下為保護自然人與確保該資料之自由流通，制定（EU）第2016/679號規則，並廢除95/46 / EC指令。

[2] These guidelines set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.
這些指引規定有關當事人行使權利之一般原則，而非考量GDPR下每個當事人權利之特定模式。

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
2016年4月27日歐洲議會與歐盟理事會通過之（EU）第2016/680號指令，係關於權責機關為預防、調查、偵查或起訴犯罪或執行刑事處罰而運用個人資料及此類資料自由流通等情事之自然人保護，並廢除第2008/977 / JHA號理事會架構決定。

則之解釋[4]。與所有WP29指引相同，本指引旨在規範與控管者相關之普遍適用情形，而非考量任何特定資料控管者之行業、產業或監管規範。因此，本指引無法就特定行業、產業或受監管領域之透明化義務提出可能的細微差別和各種變數。然而，本指引目的在使控管者能夠高度理解WP29對透明化義務在實務應用上之解釋，並表明WP29認為控管者為符合透明化所應採取之方式，並同時將公正性和課責性納入其透明化措施。

2. Transparency is a long established feature of the law of the EU[5]. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a)[6]), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles.[7] Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.[8] Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[9].

透明化是歐盟法律長期以來所建立之特點[5]，目的在於藉由使公民瞭解，或在必要時挑戰影響其權益之程序，從而使公民對該程序產生信任。透明化亦為歐盟基本權利憲章第8條所述關於個人資料運用之公正原則之展現。GDPR（第5條第1項第a款[6]）除了要求必須合法並公正地運用資料外，現在亦將透明化納入這些原則之基本方向[7]。透明化與公正性以及GDPR下新的課責性原則具有緊密關聯。且依據第5條第2項，控管者必須能夠證明

[4] While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be "lawful, fair and transparent" in relation to the natural persons concerned.
雖然透明化並非（EU）第2016/680號指令第4條關於運用個人資料的原則之一，但前言第26點指出，任何與自然人相關之個人資料運用必須是「合法、公正以及透明」的。

[5] Article 1 of the TEU refers to decisions being taken "*as openly as possible and as close to the citizen as possible*"; Article 11(2) states that "*The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society";* and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.
歐洲聯盟條約（TEU）第1條規定決定之做成「*應盡可能公開且盡可能貼近公民*」；第11條第2項規定「*各機關應與協會代表和公民社會保持公開、透明和定期之溝通*」；以及歐洲聯盟運作條約（TFEU）第15條除其他事項外，規定歐盟公民有權查閱歐盟機關、機構、辦事處和局處之文件並要求該歐盟機關、機構、辦事處和局處確保其程序之透明。

[6] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".
「與當事人相關之個人資料運用應以合法、公正和透明之方式為之」。

[7] In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).
在95/46 / EC指令中，透明化僅在前言第38點中藉由要求資料運用必須公正而間接提及，但並未在相應的第6條第1項第a款中敘明。

與當事人相關個人資料之運用是以透明的方式為之[8]。與此相關者，課責性原則要求運用作業之透明化，以便資料控管者得以證明其遵循GDPR規定之義務[9]。

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/ notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

   依據GDPR前言第171點，對於在2018年5月25日之前已進行之運用行為，資料控管者應確保截至2018年5月25日時，該運用符合其透明化義務（以及GDPR下其他所有義務）。意即，在2018年5月25日之前，資料控管者應重新審查提供予當事人有關運用其個人資料（例如隱私聲明/通知等）的所有資訊，以確保其符合本指引所討論有關透明化之要求。若對此類資訊有所變更或增補，控管者應向當事人明確說明為遵循GDPR已實施該項變更。WP29建議應主動使當事人注意此變更或增補，控管者至少應公開揭露該資訊（例如公布於網站上）。然而，若為重大或實質性的變更或增補時，依據以下第29至32段，應主動使當事人注意此變更。

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights[10]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as

[8] Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.
GDPR第5條第2項要求資料控管者依據課責性原則證明透明化（連同第5條第1項規定與資料運用相關之其他五項原則）。

[9] The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.
GDPR第24條第1項規定資料控管者有義務採取技術性和組織性措施，確保並得以證明依GDPR執行運用。

the actual content of the transparency information, which must be provided to data subjects.
當資料控管者遵守透明化義務時，能使當事人得以判斷資料控管者和受託運用者是否可課責，並透過例如：提供或撤回「告知後同意」，和行使當事人權利來掌控其個人資料[10]。GDPR下之透明化概念是以使用者而非法律為中心，並透過許多條文中對資料控管者和受託運用者的特定具體要求而得以實現。GDPR第12至14條概述了該具體（資訊）要求。然而，資訊之品質、可得性和可理解性與應提供給當事人之透明資訊的實際內容同等重要。

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:
GDPR中的透明化要求於資料運用之法律依據與整個運用過程皆有適用。第12條明確規定，透明化適用於資料運用週期之以下階段：

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
在資料運用週期之前或開始時，即：自當事人蒐集或以其他方式取得個人資料時；
- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
在整個資料運用期間，即：與當事人就其權利進行溝通時; 以及
- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.
在資料運用過程中的某些特定時點，例如在發生資料侵害或在運用行為有重大變更時。

The meaning of transparency
透明化之含義

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:
GDPR並未定義何謂透明化。GDPR前言第39點就資料運用背景下透明化原則之含義和影響提供了相關資訊：

"*It should be transparent to natural persons that personal data concerning them are collected,*

[10] See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-201/14) at paragraph 74: *"the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".*
請參閱，例如巴拉案（案例C-201/14）中佐審官克魯茲·比利隆之意見（2015年7月9日），第74段：「*要求告知當事人關於其個人資料之運用以確保所有運用之透明化，這一點尤為重要，因影響當事人行使其依據95/46指令第12條對被運用資料之近用權，及第14條之拒絕權*」。

used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"

「*個人資料之蒐集、使用、查詢或其他運用，應向該資料之自然人保持透明化，且應及於該個人資料所被運用或將被運用之程度。透明化原則要求關於個人資料運用之任何資訊或溝通方式應便於取得、易於理解且應使用清晰簡明之語言。透明化原則特別關注提供當事人控管者身分、運用資料之目的以及得以確保相關自然人資料運用之公正性和透明化的進一步資訊，並確保其有權利就受運用之個人資料進行確認和溝通。…*」

Elements of transparency under the GDPR

GDPR下透明化之要件

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13-14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

   由於GDPR下之透明化適用於當事人之權利，因此相關主要條款規範於第三章（當事人之權利）。第12條規定以下情形應適用之一般規則：向當事人提供資訊（第13-14條）；與當事人就其權利之行使進行溝通（第15-22條）；以及就資料侵害進行之溝通（第34條）。第12條特別要求相關資訊或溝通必須遵循下列規則：

   - it must be concise, transparent, intelligible and easily accessible (Article 12.1);
     必須簡潔、透明、易懂且便於取得（第12條第1項）；
   - clear and plain language must be used (Article 12.1)；
     必須使用清晰簡明之語言（第12條第1項）；
   - the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
     清晰簡明語言之要求在向兒童提供資訊時尤為重要（第12條第1項）；
   - it must be in writing "*or by other means, including where appropriate, by electronic means*"

(Article 12.1);
必須以書面形式提供，「*或透過其他方式，包括在適當情況下，透過電子方式提供*」（第12條第1項）；

- where requested by the data subject it may be provided orally (Article 12.1) ; and
  若當事人提出要求，得以口頭提供資訊（第12條第1項）；以及
- it generally must be provided free of charge (Article 12.5).
  一般情形下必須無償提供資訊（第12條第5項）。

"Concise, transparent, intelligible and easily accessible"
「簡潔、透明、易懂且便於取得」

8. The requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.
   向當事人提供資訊和進行溝通之方式應「簡潔和透明」之要求，意味著資料控管者應該有效率地和簡潔地提供資訊/溝通，以避免資訊疲勞。此類資訊應和其他非隱私相關資訊（如契約條款或一般使用條款）做出明確之區分。在網路環境中，使用階層隱私聲明/通知將能夠引導當事人至其想要立即取得隱私聲明/通知之特定部分，而不需瀏覽大量文本以搜尋特定之項目。

9. The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.
   資訊需「易於理解」之要求意味著該資訊應能夠被目標群眾的一般成員所理解。可理解

性與使用清晰簡明語言之要求密切相關。可歸責之資料控管者將會知悉其蒐集資料之當事人，並可使用這些資訊來確認群眾可能理解之內容。例如，蒐集專業工作人員個人資料之控管者可以假設其目標群眾比蒐集兒童個人資料之控管者具有更高之理解程度。若控管者不確定資訊的可理解性和透明化以及用戶介面/通知/政策等的有效性，控管者可透過某些機制加以測試，例如，透過用戶面板、可讀性測試、正式和非正式互動以及與產業團體、消費者權益保護團體和監管機關進行對話溝通，或酌情使用其他機制。

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that *"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data..."* In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important *consequences* of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.

這些條款中概述之透明化原則的核心考量在於，當事人應能夠事先確認所需運用的資料範圍及後果為何，而不至於日後某一時點因其個人資料被使用之方式而感到意外。此亦為GDPR第5條第1項所規定公正原則下的一個重要面向，且與前言第39點相關，該前言指出「*應使自然人了解關於運用個人資料之風險、規則、安全維護措施和權利...*」。特別是對複雜的技術性或未預期之資料運用，WP29的立場與依據第13條和第14條提供前述資訊（本指引將於其後另做說明），控管者亦應使用明確的語言單獨說明該運用將產生的最重要*後果*：易言之，隱私聲明/通知中所描述之具體運用對當事人實際上會產生何種影響？依據課責性原則以及前言第39點，資料控管者應評估是否有涉及此類運用之自然人應注意之特殊風險。此方式有助於全面釐清可能對當事人在與保護其個人資料相關之基本權利和自由方面產生最大影響的資料運用類型。

11. The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be

accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

「便於取得」之要件意味著當事人無需搜尋；此類資訊於何處取得及如何取得，對當事人而言應立即且明顯，例如直接提供、透過連結、透過明確指示或以一般用語問答（例如，於網路分層的隱私聲明/通知中、於常見問題解答(FAQs)中、於當事人網路填寫表格時彈出視窗、或於互動式數位聊天機器人界面等。這些機制於以下第33至40段進一步考量）。

Example

示例

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as “Privacy”, “Privacy Policy” or “Data Protection Notice”). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

每個經營網站的組織都應在其網站上公布隱私聲明/通知。隱私聲明/通知的直接連結應在該網站的每個頁面上以常用術語（例如「隱私」、「隱私政策」或「資料保護通知」）清楚表明。若因擺放位置或配色方式使內容或網址連結不明顯或難以在網頁上發現，則將認為其不便於取得。

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than “two taps away” (e.g. by including a “Privacy”/ “Data Protection” option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

對於行動應用程式，相關必要資訊應在下載前從網路商店取得。應用程式安裝後，相關資訊仍需易於該程式取得。滿足此項要件方式之一係確保無須「點擊超過兩次」以取得資訊（例如透過在應用程式功能表中建立「隱私」/「資料保護」選項）。此外，該隱私資訊應針對特定應用程式，而非僅為擁有或向公眾提供該應用程式之公司的一般隱私政策。

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.

WP29建議，實務最佳做法是，於線上蒐集個人資料同時，應提供隱私聲明/通知之連結，或在蒐集個人資料的同一頁面上提供該資訊。

"Clear and plain language"

「清晰簡明之語言」

12. With *written* information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed.[11] A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator[12] and is also explicitly referred to in the context of consent in Recital 42 of the GDPR[13]. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

    提供書面資訊（以及口頭傳遞書面資訊，或透過影音/視聽之方式，包括對視力受損之當事人），應遵循明確書寫之最佳實務做法[11]。歐盟立法者[12]曾使用過類似的語言要求（對於「簡明易懂之語言」），而GDPR前言第42點中，在有關同意之規範也明確提及了該項要求[13]。對清晰和簡明語言之要求意味著應盡可能以簡單的方式提供資訊，避免複雜的句子和語言結構。資訊應具體而明確；且不應以抽像或矛盾之措辭來表達，也不應留有做出不同解釋之空間。特別是運用個人資料之目的和法律依據必須是清楚的。

[11] See How to Write Clearly by the European Commission (2011), to be found at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.
請參閱由歐盟執委會發行之如何明確書寫（2011），請查閱：https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
1993年4月5日理事會第93/13 / EEC號指令第5條有關消費者契約中不公正之條款。

[13] Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.
前言第42點指出，資料控管者預先制定之同意聲明應以易於理解和易於取得之形式為之，且應使用清晰簡明之語言，且不應包含不公正之條款。

Poor Practice Examples

不良實務示例

The following phrases are not sufficiently clear as to the purposes of processing:

下列語句就於運用目的之解釋不夠明確：

- *"We may use your personal data to develop new services"* (as it is unclear what the "services" are or how the data will help develop them);

  「*我們可能會使用您的個人資料來開發新服務*」（該「服務」為何或該資料將如何協助開發皆不明確）；

- *"We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and

  「*我們可能會將您的個人資料用於研究目的*」（該「研究」為何並不明確）；及

- "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails).

  「*我們可能會使用您的個人資料以提供個人化服務*」（何謂「個人化」並不明確）。

Good Practice Examples[14]

優良實務示例[14]

- "*We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in* " (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);

  「*我們將保留您的購物歷史記錄並使用您之前購買產品的詳細資訊，以便為您提供我們認為您也會感興趣其他產品之建議*」（此語句清楚表示將運用何種類型之資料、當事人將成為精準廣告對象且其資料將用於達到此目的）；

[14] The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.

對透明化之要求完全獨立於依據第6條資料控管者需確保資料運用有適當法律依據之要求。

- "*We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive*" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and

  「*為了瞭解用戶如何使用我們的網站，以便我們可以改善網站的直觀性，我們將保留和評估您最近造訪我們網站之資訊以及就您於網站上點選不同區塊之行為進行分析。*」（此語句清楚表示將運用何種類型之資料以及控管者將進行何種類型之分析）；及

- "*We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read*" (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

  「*我們將會記錄您所點擊之本網站文章，依據您所閱讀的文章等相關資訊辨識出您的興趣，並於本網站對您提供精準行銷*」（清楚表示個人化所需為何，以及如何辨識當事人之興趣）。

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets[15] data subjects speaking those languages.)

    另應避免使用諸如「可能」、「也許」、「某些」、「經常」和「或許」之語言後置修飾語。若資料控管者選擇使用此種不確定語言，依據課責性原則，控管者應要能夠證明

無法避免使用該語言之原因以及如何不損害運用之公正性。段落和句子之結構應該合理，並利用項目符號和縮排來顯示階層關係。應以主動式而非被動式書寫，且應該避免使用過多的名詞。提供給當事人之資訊不應包含過多法律、技術或專業語言或術語。當資訊被翻譯成一種或多種語言時，資料控管者應確保所有翻譯皆為準確的，且用語和語法在第二種語言中是合理的，使翻譯之內容不需被闡釋或重新解釋。（當控管者針對[15]的當事人使用某些語言時，控管者應提供一種或多種其他語言之翻譯。）

Providing information to children and other vulnerable people

向兒童和其他弱勢群體提供資訊

14. Where a data controller is targeting children[16] or is, or should be, aware that their goods/ services are particularly utilised by children (including where the controller is relying on the consent of the child)[17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them.[18] A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".[19]

當資料控管者以兒童[16]為對象，或是（或必須）知悉兒童使用其商品/服務之情形（包括控管者需獲得兒童之同意時）[17]，控管者應確保所使用語言之詞彙、語氣和風格需適合兒童並可與其產生共鳴，以使接收該資訊之兒童可意識到該訊息/資訊是直接對其所為。[18]「聯合國兒童友好語言之兒童權利公約」提供了一種以兒童為中心的語言以替代原始法律語言之範例。[19]

---

[15] For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.
例如，當控管者以系爭之語言經營網站和/或提供特定國家選項和/或提供以特定成員國之貨幣支付商品或服務之情形下，這些皆可作為資料控管者針對特定成員國當事人之指標。

[16] The term "child" is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years.
GDPR並未定義「兒童」一詞，但WP29認為，依據所有歐盟成員國簽署之「聯合國兒童權利公約」，兒童係指未滿18歲之人。

[17] i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).
即16歲或16歲以上之兒童（或依據GDPR第8條第1項，成員國國家法律就兒童對於資訊社會服務之同意設立介於13歲至16歲間的特定年齡門檻，而該兒童達到該國家法定同意年齡）。

[18] Recital 38 states that "Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". Recital 58 states that "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand".
前言第38點指出「有鑑於兒童可能未盡知悉其個人資料運用之風險、後果及相關安全維護措施與其權利，兒童就其個人資料應受到特別保護」。前言第58點指出「有鑑於兒童應受到特別保護，任何提供予兒童之資訊及溝通應採用兒童易於理解之清晰簡明之語言」。

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

15. WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds.[20] It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age,[21] Article 8 *does not provide* for transparency measures to be directed at the holder of parental responsibility who gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.

WP29之立場為，透明化是一種獨立的權利，同等適用於兒童及成年人。WP29特別強調，兒童不會因在GDPR第8條適用之情況下，由於法定代理人所給予或授權同意，而失去身為資料當事人所擁有之透明化權利。雖然在許多情況下，此種同意將由法定代理人一次性給予或授權，但兒童（如同其他當事人）在與控管者互動的整個過程中，始終享有透明化之權利。這符合「聯合國兒童權利公約」第13條，該條規定兒童有言論自由之權利，包括尋求、接受和傳播各類資訊和思想之權利。[20]必須指出，雖然第8條並未針對一定年齡下兒童自己所為之同意[21]，就給予此類同意權之法定代理人訂定透明化措施。因此，依據第12條第1項中針對兒童透明化措施之特定要求（前言第38點和第58點亦支持），當資

[20] Article 13 of the UN Convention on the Rights of the Child states that: "The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."
聯合國兒童權利公約第13條規定：「兒童應享有言論自由之權利；此權利包括尋求、接受和傳播各類資訊和思想之自由，不分國界，無論是以言詞、書面或印刷、藝術形式，或透過兒童選擇之其他媒介。」

[21] See footnote 17 above.
請參閱前註17。

料控管者是針對兒童，或知悉其商品或服務是由識字年齡兒童使用時，其有義務確認任何資訊和溝通都應以清晰簡明的語言或兒童可輕易理解之媒介傳達。然而，為避免爭議，WP29認為，對於年紀很小或尚不識字的兒童，亦可向法定代理人提供透明化措施，因在大多數情況下，即使是最基本之書面或非書面關於透明化的訊息，這些兒童也不太可能理解。

16. Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.[22] This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.

同樣，若資料控管者知悉其商品/服務是由（或針對）社會其他弱勢成員（包括身心障礙人士或可能難以獲得資訊之人）所使用，在評估如何確保其符合與當事人相關之透明化義務時，控管者應考量此類型當事人之易受傷害性。[22]如前文第9段所述，此與資料控管者評估其目標受眾可能之理解程度相關。

"In writing or by other means"

「以書面或其他方式」

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing.[23] (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified "means" including electronic means to be used. WP29's position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37).[24] However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information

[22] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.
例如，「聯合國身心障礙者權利公約」要求向身心障礙者提供適當形式之援助和支持，以確保其獲得資訊。

to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of *methods* to ensure transparency in relation to processing.

依據第12條第1項，向當事人提供資訊或溝通之基本方式係以書面為之。[23]（第12條第7項亦規定了與標準化圖示一併提供之資訊，此議題將於第49至53段關於視覺化工具部分另加說明）。然而，GDPR亦允許使用其他未指明之「方式」，包括使用電子方式。WP29對書面電子方式之立場為，當在資料控管者經營（或其營運係部分或全部透過）網站之情況下，WP29建議使用分層隱私聲明/通知，允許網站使用者可瀏覽其最感興趣的相關隱私聲明/通知（有關分層隱私聲明/通知的進一步資訊請參閱第35至37段）。[24]然而，提供予當事人之全部資訊應放置於同一個位置或以一份完整之文件呈現（無論係數位或紙本格式），使當事人欲查看整份文件時，即可以輕鬆地取得所提供之資訊。重要的是，分層方式的使用不僅限於以書面電子方式向當事人提供資訊時。如以下第35至36段和第38段所述，選擇使用各種*方式*之組合來確保關於運用的透明化時，亦可遵循分層方式向當事人提供資訊。

18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used *in addition* to a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts.[25] "Other means", which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

當然，數位分層隱私聲明/通知並非控管者可使用的唯一書面電子方式。其他電子方式包括「即時」上下文彈出通知、3D觸碰或滑鼠游標懸停通知（hover-over notices）以及隱私儀表板（privacy dashboards）。除了分層隱私聲明/通知*以外*，可使用之非書面電子方式亦可包括影音和智能手機或物聯網（IoT）語音警示。[25]「其他方式」並非一定為電子方式，亦可包括如卡通、資訊圖表或流程圖。當透明化資訊是專門針對兒童之情況下，控

[23] Article 12.1 refers to "language" and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.
第12條第1項提及「語言」，並指出資訊應以書面或其他方式提供，包括在適當情況下以電子方式提供。

[24] The WP29's recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.
WP29對階層通知益處之認可已展現於第10/2004號關於更協調之資訊條款意見及第02/2013號關於智能設備上之行動應用程式意見。

[25] These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.
這些電子方式之示例僅供參考，資料控管者可發展創新方式以符合第12條之規範。

管者應考量何種類型之措施特別適合兒童使用（例如可能包括漫畫/卡通、圖像以及動畫等其他措施）。

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject's information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative *additional* means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things[26] (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

重要的是，選擇提供資訊之方式需符合特定情況，即資料控管者和當事人互動之方式或蒐集當事人資訊之方式。例如，若蒐集個人資料之設備並無螢幕（例如物聯網設備/智能設備）以供造訪網站/顯示書面資訊，則僅提供電子書面格式之資訊（例如網路隱私聲明/通知）可能不適合/不可行。在此情況下，應考量*其他*適當之替代方式，例如在紙本說明手冊中提供隱私聲明/通知，或在紙本說明書或外包裝提供網路隱私聲明/通知的URL網址（即網站上之特定頁面）。若該無螢幕之設備具有語音功能，則亦可另以語音（口頭）提供相關資訊。WP29先前在其關於物聯網近期發展意見書中[26]曾就透明化和提供當事人資訊提出建議（例如使用刊印在物聯網物件上之QR碼，當掃描該QR碼時，將顯示所需之透明化資訊）。此建議於GDPR仍有適用。

"..the information may be provided orally"

「..得以口頭提供資訊」

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are

[26] WP29 Opinion 8/2014 adopted on 16 September 2014
WP29第8/2014號意見於2014年9月16日通過。

a specific named person and the means should enable the controller to verify a data subject's identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to *future* users/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under Articles 13 and 14 may be provided by oral means without the controller requiring a data subject's identity to be proven.

第12條第1項特別考量若當事人之身分可透過其他方式確認，得應當事人之要求向其口頭提供資訊。易言之，所採行之方式不得僅基於當事人聲稱其為該特定人士，且該方式應使控管者得充分核實當事人之身分。在口頭提供資訊前需核實當事人身分之要求僅適用於當該資訊與特定當事人依據第15條至第22條和第34條行使其權利有所關聯時。提供口頭資訊之先決條件不適用於第13條和第14條所規範一般隱私資訊之提供，因第13條和第14條所要求之資訊亦需提供予未來的用戶/客戶（資料控管者無法核實其身分）。因此，依第13條和第14條規定所應提供之資訊，得未經控管者核實當事人之身分，以口頭方式提供。

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject's identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

第13條和第14條所規範之口頭提供資訊並非必須以人對人之方式為之（即親自或透過電話）。除書面方式外，亦可提供自動口頭資訊。例如，當視力受損之人與資訊社會服務提供者互動時或如前文第19段所述智能設備並無螢幕時，即可適用此種方式。若資料控

管者選擇以口頭提供資訊予當事人，或當事人要求提供口頭資訊或溝通，WP29之立場為資料控管者應允許當事人可重複聽取預先錄製之資訊。當口頭資訊之要求涉及有視覺障礙之當事人或涉及可能難以書面形式獲得或理解資訊之其他當事人時，此要件係為必要的。資料控管者另應確保其擁有下列紀錄並可提出證明（以符合課責性之要求）：（i）以口頭方式提出資訊之要求，（ii）核實當事人身分之方式（如適用 – 請參閱前文第20段）以及（iii）向當事人提供資訊之事實。

"Free of charge"

「無償」

22. Under Article 12.5,[27] data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects).[28] This aspect of transparency also means that any information provided under the transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods.[29]

第12條第5項規定[27]，資料控管者一般不得對依據第13條和第14條所應提供予當事人之資訊，或依據第15-22條（關於當事人的權利）及第34條（就個人資料侵害與當事人進行溝通）採取之溝通和行動收取費用。[28]透明化之此點要素也表示依據透明化要求提供之任何資訊皆不得以交易為條件，例如支付或購買服務或貨物。[29]

Information to be provided to the data subject – Articles 13 & 14

應提供予當事人之資訊 - 第13條和第14條

---

[27] This states that "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."
該條款規定「依據第13條和第14條提供之資訊以及依據第15條至第22條和第34條所採取之任何溝通和任何行動均應無償提供。」

[28] However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).
然而，依據第12條第5項，例如當事人就第13條和第14條規定之資訊或第15條至第22條或第34條規定之權利所提出之請求過度或明顯無依據時，控管者可收取合理之費用。（此外，關於第15條第3項近用之權利，若當事人要求任何進一步的個人資料副本，控管者得基於行政成本收取合理費用）。

[29] By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained".
舉例來說，若有關當事人個人資料之蒐集與購買行為相關，依據第13條要求提供之資訊則應在付款前以及蒐集資料時提供，而非在交易結束後。同樣，在向當事人提供免費服務之情況下，第13條之資訊必須在註冊前而非註冊後提供，因第13條第1項要求資訊之提供需「在取得個人資料時」。

Content

內容

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The **table in the Annex** to these guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.

GDPR列舉出有關當運用當事人之個人資料係從當事人取得（第13條）或從其他來源蒐集（第14條）時，必須提供予當事人之資訊類型。本指引**附錄表格**綜整了依據第13條和第14條必須提供之資訊類型，亦將這些要求之性質、範圍和內容納入考量。為臻明確，WP29之立場為，第13條和第14條的第1項及第2項下所應提供之資訊情狀並無區別。這些項次中的所有資訊皆具有同等重要性，且必須提供予當事人。

"Appropriate measures"

「適當之措施」

24. As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller's responsibility to take "appropriate measures" in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/ service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.

除內容外，依第13條和第14條要求應提供予當事人之資訊的格式和方式亦同等重要。包含此類資訊之通知一般被稱作資料保護通知、隱私通知、隱私政策、隱私聲明或公正運

用通知。GDPR並未規定應向當事人提供此類資訊之格式或形式，但明確規範資料控管者有責任依透明化目的就所需提供之資訊採取「適當措施」。此意味著資料控管者在決定提供資訊之適當格式或形式時，應考量資料蒐集和運用的所有情狀。尤其是，必須依據產品/服務用戶體驗以評估適當之措施。此意味著應考量所使用之設備（如適用）、用戶界面/與控管者互動之性質（用戶「旅程」）以及這些情況所產生之限制。如前文第17段所述，WP29建議，若資料控管者擁有網路平台，則應提供網路分層隱私聲明/通知。

25. In order to help identify the most appropriate modality for providing the information, in advance of "going live", data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardised tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances.
為了協助確認提供資訊最合適之方式，在「上線」之前，資料控管者可能希望透過用戶測試（例如，廳堂測試（hall tests）或其他可閱讀性或可造訪性之標準化測試），嘗試不同模式，以尋求有關用戶可造訪性、易理解性和易使用性建議措施之回饋意見。（請另參閱前文第9段關於進行用戶測試之其他機制的進一步評論）。記錄此類嘗試可使資料控管者展示在特定情況下已選擇最適當傳達資訊之工具/方式，以協助資料控管者履行其課責性之義務。

Timing for provision of information
提供資訊之時點

26. Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle[30]. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:
第13條和第14條規定必須在資料運用週期的開始階段向當事人提供資訊[30]。第13條適用於從當事人蒐集資料之情況。包含當個人資料：

- a data subject consciously provides to a data controller (e.g. when completing an online form);

[30] Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.
依據公正和目的限縮原則，從當事人蒐集個人資料之組織應在蒐集時即具體說明運用之目的。若其目的包括建立推定性個人資料（inferred data）、企圖建立並進一步運用此類推定性個人資料以及將運用的推定資料之類別，控管者必須在蒐集時或依據第13條第3項或第14條第4項基於新目的而欲進階運用個人資料前，就其目的與當事人進行溝通。

or

係當事人有意識地提供給資料控管者（例如，當完成網路表格時）；或

- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

  係資料控管者透過觀察從當事人蒐集（例如，使用自動資料獲取設備或資料獲取軟體，例如相機、網路設備、Wi-Fi跟踪、無線射頻辨識（RFID）或其他類型之感應器）。

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:

第14條適用於非從當事人取得資料之情況。此包括資料控管者由以下來源取得個人資料：

- third party data controllers; 第三方資料控管者；
- publicly available sources; 公眾來源；
- data brokers; or 資料仲介；或
- other data subjects. 其他當事人。

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided *"at the time when personal data are obtained"*. In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:

    有關提供資訊的時間，及時提供這些資訊是透明化義務和公正運用資料義務的關鍵要素。在適用第13條之情況下，依據第13條第1項，必須「*在取得個人資料時*」提供資訊。在依據第14條間接取得個人資料之情況下，必須向當事人提供所需資訊的時間範圍，依第14條第3項第a至c款規定如下：

    - The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, *"having regard to the specific circumstances in which the personal data are processed"* (Article 14.3(a)).

      一般要求為，必須在取得個人資料後的「合理期限」內提供資訊，且不得遲於一個月，「*考量到運用個人資料之具體情狀*」（第14條第3項第a款）。

    - The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b),[31] which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided at the latest at the time of the first communication with the data subject. If the first communication occurs prior to the

one-month time limit after obtaining the personal data, then the information must be provided *at the latest* at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

第14條第3項第a款規定之一個月期限，於資料係用於與當事人溝通之情況下，依據第14條第3項第b款得加以縮減[31]。於此情形下，最遲須在與當事人進行第一次溝通時提供資訊。若第一次溝通發生在取得個人資料後的一個月期限內，則*最遲*必須在第一次與當事人溝通時提供資訊，即使從取得資料開始的一個月期限尚未到期。若第一次溝通發生在取得個人資料後之一個月後，則仍應適用第14條第3項第a款，因此第14條之資訊最遲須在取得資料的一個月內提供予當事人。

- The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c)[32] which provides for a situation where the data are being disclosed to another recipient (whether a third party or not)[33]. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided *at the latest* at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

  第14條第3項第a款規定之一個月期限，於資料向另一接收者(無論是否為第三方)[32]揭露時，依據第14條第3項第c款規定得加以縮減[33]。於此情形下，必須最遲在第一次揭露時提供資訊。若揭露發生於一個月期限之前，則*最遲*必須在第一次揭露時提供資訊，即使從取得資料開始的一個月期限尚未屆至。與第14條第3項第b款之立場相似，若在取得個

[31] The use of the words *"if the personal data are to be used for.."* in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
在第14條第3項第b款中使用「*若個人資料用於...*」一詞，表示對第14條第3項第a款規定最長期限一般立場之特定情況說明，而非替代之。

[32] The use of the words *"if a disclosure to anther recipient is envisaged..."* in Article 14.3(c) likewise indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
在第14條第3項第c款中使用「*若預計向他人揭露個人資料...*」一詞，同樣表示對第14條第3項第a款規定最長期限一般立場之特定情況說明，而非替代之。

[33] Article 4.9 defines "recipient" and clarifies that a recipient to whom personal data are disclosed does not have to be a third party. Therefore, a recipient may be a data controller, joint controller or processor.
第4條第9款定義何謂「接收者」，並闡明揭露個人資料之接收者不一定為第三方。因此，接收者亦可為資料控管者、共同控管者或受託運用者。

人資料一個月後始發生個人資料之揭露，則第14條第3項第a款仍繼續適用，因此第14條之資訊最遲須在取得資料的一個月內提供予當事人。

28. Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be *"made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing".* Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

因此，在任何情況下，必須向當事人提供第14條資訊之最長期限為一個月。然而，在決定提供第14條資訊之時點時，GDPR之公正和課責原則要求資料控管者隨時考量當事人之合理期待、該項運用對當事人之影響以及當事人就該運用得以行使之權利。課責性要求控管者證明其決定之理由及於某時點提供資訊之正當性。實際上，於「最後時點」提供資訊可能難以符合上述要求。有鑑於此，前言第39點敘明，除其他事項外，應使當事人「*知悉與運用個人資料相關之風險、規則、安全維護措施和權利，以及如何行使和此類運用相關之權利*」。前言第60點亦提及在公正和透明化運用原則背景下，應向當事人通知運用作業的存在及其目的。基於以上原因，WP29之立場為，在可能的情況下，依據公正原則資料控管者應提前於規定期限內妥為向當事人提供資訊。關於就運用作業通知當事人與實際發生此類運用作業之間的適當時間點，在第30至31段和第48段中有進一步說明。

Changes to Article 13 and Article 14 information

第13條和第14條資訊之變更

29. Being accountable as regards transparency applies not only at the point of collection of

personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the change would be to data subjects. Changes to a privacy statement/ notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation to the processing. Conversely, an example of changes to a privacy statement/ notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/ grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(A). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

對透明化之課責性不僅適用於蒐集個人資料時，且適用於整個資料運用過程，無論傳達之資訊或溝通為何。例如，更改現有隱私聲明/通知內容之情形。在溝通最初的隱私聲明/通知及對該聲明/通知為任何後續實質或重大變更時，控管者皆應遵循相同之原則。控管者在評估何謂實質或重大變更時，應考量之因素包含：對當事人之影響（包括其行使權利之能力），以及當事人對該變更感到意外/訝異之程度。必須與當事人進行溝通的隱私聲明/通知變更包括：運用目的之變更；控管者身分之變更；或當事人行使與資料運用相關權利之變更。反之，某些變更並非WP29所認為之實質或重大的隱私聲明/通知變更，例如包括錯誤拼寫或文體/文法瑕疵之更正。由於大多現有客戶或用戶僅會快速瀏覽隱私聲明/通知變更之通知，因此控管者應採取一切必要措施，以確保傳達之方式可使大多數

收件人實際注意到該變更。此意味著，例如，以適當的方式（例如：電子郵件、書面信件、彈出頁面或其他能有效引起當事人注意之方式），專門針對該變更進行通知(例如：該通知與行銷內容分開)，且傳達方式需符合第12條要求之簡潔、透明、易懂、易於取得和使用清晰簡明之語言。僅於隱私聲明/通知中提及當事人應定期檢查隱私聲明/通知之變更或更新，不僅將被視為不充足，亦不符合第5條第1項第a款中之公正性。有關通知當事人變更之時點的其他指導請參閱以下第30至31段。

Timing of notification of changes to Article 13 and Article 14 information
通知第13條和第14條資訊變更之時點

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 45). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).

GDPR對於原依第13條或第14條(除意圖為其他目的之運用外。該情形下，依第13條第3項及第14條第4項，應於開始運用前即為通知—請參閱以下第45段)提供予當事人之資訊變更時，通知當事人該項變更之時點要求（及方式）並無規定。然而，如前文關於第14條資訊提供時點中所述，資料控管者必須再次考量在公正性和課責性原則下，當事人的任何合理期待或該項變更對當事人造成之潛在影響。若資訊之變更顯示運用的本質發生根本的變化（例如擴大接收者之類別或將傳輸至第三國）或雖變更對運用作業並無根本性之影響，但也許與當事人相關並對其產生影響，則這些資訊應在變更實際生效前完整地提供予當事人，且用於使當事人注意到該變更之方式必須係清楚且有效的。如此是為了確保當事人不至「錯過」變更，且使其在合理的時間範圍內得（a）考量該變更之本質

和影響，以及（b）行使其在GDPR下關於該變更之權利（例如撤回同意或拒絕運用）。

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the change taking effect satisfies the principle of fairness to the data subject. Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.

資料控管者應仔細考量透明化下所需提供更新資訊的每種情狀和背景，包括變更對當事人的潛在影響以及用於傳達該項變更之方式，並得以證明變更通知和變更生效之間的時間如何符合對當事人之公正原則。此外，WP29的立場為，與公正原則一致，在向當事人通知此類變更時，資料控管者亦應說明該變更對當事人可能產生之影響。然而，符合透明化要件並無法「掩飾」該項運用之重大變更，已導致該運用在本質上已與之前完全不同。WP29強調，GDPR中其他所有的規則，包含與其他運用不相容之相關規則，無論是否符合透明化義務，皆繼續適用。

32. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/ notice and where they can find it.

此外，即使透明化資訊（例如隱私聲明/通知中包含之資訊）並無重大變更，但於長時間使用服務後，當事人已無法回憶起最初依據第13條和/或第14條所提供之資訊。WP29建議控管者應使當事人能持續輕鬆取得該資訊，以便重新了解資料運用之範圍。依據課責性原則，控管者亦應考量是否以及間隔多長時間後，適合明確提醒當事人關於隱私聲明/通知之資訊，及可於何處找到該資訊。

Modalities - format of information provision

提供方式 – 提供資訊之格式

33. Both Articles 13 and 14 refer to the obligation on the data controller to *"provide the data subject with all of the following information..."* The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

第13條和第14條皆提及資料控管者有義務「*向當事人提供以下所有資訊...*」。此處之關鍵詞為「提供」。此意味著資料控管者必須採取積極之步驟向當事人提供相關資訊，或主動將當事人引導至資訊所在位置（例如，透過直接連結，使用QR碼等）。當事人無須主動在其他資訊中（例如網站或應用程式中的使用條款和條件）搜尋這些條款所涵蓋之資訊。相關說明請參閱第11段中之示例。如前文第17段所述，WP29建議，提供予當事人之全部資訊應放置於同一個位置或以一份完整之文件呈現（無論是在網頁上的數位資訊或紙本），使當事人欲查閱整份文件時，即可以輕鬆地取得。

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.

GDPR的規範存在著本質上的緊張關係，一方面GDPR要求向當事人提供全面性之資訊，另一方面要求以簡潔、透明、易懂且便於取得之形式為之。因此，控管者應本於課責性和公正性的基本原則，就其執行及決定個人資料運用之本質、情況、範圍和背景自行分析，於GDPR的法律要求範圍內並考量本指引中之建議(特別是第36段)，決定必須提供予當事人資訊之優先順序，以及傳達資訊的適當詳細程度和方式。

Layered approach in a digital environment and layered privacy statements/ notices

數位環境中之分層方式和分層隱私聲明/通知

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

在數位環境中，考量到需要提供給當事人之資訊量，資料控管者在選擇使用各種方式之組合來確保透明化時，可採用分層方式。WP29特別建議，分層隱私聲明/通知應使用連結方式，至須提供給當事人之各類資訊，而非僅在螢幕上單一通知中顯示所有相關資訊，以避免資訊疲勞。分層隱私聲明/通知有助於解決完整性和理解性間之緊張關係，特別是可引導用戶直接到所欲閱讀之聲明/通知部分。另應注意，分層隱私聲明/通知並非須經多次點擊始能獲得相關資訊之嵌套頁面（nested pages）。隱私聲明/通知的第一層設計和版面，應使當事人能就運用其個人資料可取得之相關資訊有清楚之概觀，以及在何處/如何於隱私聲明/通知的各個階層中找到詳細資訊。同等重要者為，於分層通知中不同層級所包含之資訊須具有一致性，且不應提供相衝突之資訊。

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital

39.[34] While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

WP29於控管者以分層方式通知當事人之第一種形式內容(亦即控管者首次與當事人接觸之主要方式），或分層隱私聲明/通知第一層之內容，建議第一層/形式應包含運用目的之詳細資訊、控管者之身分和當事人權利之描述。（此外，該資訊應在蒐集個人資料時直接引起當事人之注意，例如，於當事人填寫網路表格時顯示。）前言第39點尤其強調預先提供該資訊之重要性。[34] 雖然控管者基於課責性必須能夠證明其如何決定資訊之優先性，但WP29之立場為，依據公正原則，除本段以上詳述之資訊外，第一層/形式亦應包含對當事人產生重大影響或使其感到意外之運用的相關資訊。因此，當事人應能夠從第一層/形式包含之資訊中理解相關之資料運用將對其產生之後果（亦請參閱前文第10段）。

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use *additional* transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

在數位環境中，除了提供網路的分層隱私聲明/通知外，資料控管者亦可選擇使用*其他*透明化工具（請參閱以下其他示例），為個別當事人就其關切之特定位置以及所使用之商品/服務，提供客製化之資訊。然而，應需注意，雖然WP29建議使用網路的分層隱私聲明/通知，但該建議並不排除發展和使用其他符合透明化要求之創新方式。

Layered approach in a non-digital environment

[34] Recital 39 states, on the principle of transparency, that "That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."
透明化原則，前言第39點指出，「該原則特別涉及應提供給當事人關於控管者身分和運用目的之資訊，以及用於確保對相關自然人資料運用之公正與透明化，並確保當事人有權利就其所被運用之個人資料進行確認和溝通。」

非數位環境下之分層方式

38. A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.

以分層方式向當事人提供之透明化資訊亦可使用於離線/非數位環境中（即真實世界環境，例如人對人交流或電話溝通），資料控管者可使用不同類型之方式，以便於提供資訊。（有關提供資訊之不同方式，請另參閱第33至37段和第39至40段。）然不應將此模式與分層隱私聲明/通知之個別問題相混淆。無論在此種分層方式中使用何種格式，WP29建議第一「層」（亦即控管者首次與當事人接觸之主要方式）通常應傳達最重要之資訊（如上文第36段所述），即運用目的之細節、控管者之身分和當事人所擁有之權利，以及運用產生之最大影響或可能使當事人感到意外之運用。例如，第一次與當事人係透過電話聯繫，則可在與當事人通話期間提供此類資訊，並可透過進一步且不同之方式，權衡第13/14條之要求，向其提供相關資訊，例如透過電子郵件傳送隱私政策副本和/或寄送控管者網路分層隱私聲明/通知之連結予當事人。

"Push" and "pull" notices

「推播」和「索取」式通知

39. Another possible way of providing transparency information is through the use of "push" and "pull" notices. Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, privacy dashboards and "learn more" tutorials. These allow for a more user-

centric transparency experience for the data subject.

另一種提供透明化資訊可能之方式為使用「推播」和「索取」式通知。推播通知涉及提供「即時」透明資訊通知，而「索取」通知則透過如權限管理、隱私面板和「了解更多」等方式便利資訊之取得。這些方式為當事人提供了更加以用戶為中心之透明化體驗。

- A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of demonstrating that 'privacy information' is a necessary and integral part of a service rather than a lengthy list of legalese.

  隱私面板是一個單一接觸點，當事人可查看「隱私資訊」並藉由允許或防止相關服務以特定方式運用其資料管理其隱私偏好選項。若當事人在各種不同設備上使用相同服務時，此方式特別有效，因無論其如何使用該服務，皆可控制自身之個人資料。允許當事人透過隱私面板自行手動調整其隱私設定亦可反映針對該特定當事人而發生之運用類型，以使隱私聲明/通知更加個人化。將隱私面板整合至現有服務架構中（例如，透過使用與其他服務相同之設計和品牌）應屬首選，因為如此可確保面板之造訪和使用具有直觀性，且可有助於鼓勵用戶參與這些資訊，如同參與其他服務一般。此為一種有效的方式以證明「隱私資訊」係服務必要和不可或缺之一部分，而非冗長之法律術語列表。

- A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.

即時通知係當與當事人最為相關之訊息需要其讀取時，以特別的方式提供特定之「隱私資訊」。此方式對於在整個資料蒐集過程中的各個時點提供資訊十分有用；該方式有助於將資訊之提供分散至易於瞭解之區塊，並減少對包含難以理解的關聯資訊之單一隱私聲明/通知的依賴。例如，若當事人於網路購買產品，則可在伴隨相關文字的彈出視窗中提供簡要之解釋性資訊。請求當事人提供電話號碼的文字旁即可說明例如「僅為與該購買相關之聯絡目的而蒐集該資料，且該資料僅會於遞送服務時揭露」。

Other types of "appropriate measures"

其他類型之「適當措施」

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29's position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/ online presence, is to do so through an electronic privacy statement/ notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence) use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

有鑑於歐盟網路使用之高普及性，以及當事人可隨時從多個地點和不同設備連接至網路，如上所述，WP29之立場為，若在資料控管者設有數位/網路平台之情況下，提供透明化資訊之「適當措施」應透過電子隱私聲明/通知為之。然而，基於資料蒐集和運用之情狀，資料控管者可能需要另外（或在資料控管者不擁有任何數位/網路平台之情況下）使用其他方式和格式來提供資訊。其他因以下不同之個人資料情境可能向當事人傳達資訊之方式，可能包含可適用於以下所列相關情境之模式。如上所述，當控管者選擇組合使用這些方式以確保與當事人的第一種溝通形式傳達最重要之資訊(請參閱第36、38段)時，其可能使用分層方式為之。

a. Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;

書面/紙本情境，例如透過郵寄方式簽訂契約時：書面說明、傳單、契約文件中之資訊、漫畫、資訊圖表或流程圖；

b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;
電話情境：由真人口頭說明，藉由互動和提問得到解答，或以自動或預先錄製之資訊，提供聽取更多詳細資訊之選項；

c. Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;
無螢幕智能技術/物聯網情境，如Wi-Fi追蹤分析：圖示、QR碼、語音警示、併入紙本安裝指引中之詳細說明、數位安裝指引中之影音、智能設備上之書面資訊、透過短訊或電子郵件發送之資訊、顯示板包含之資訊、公共看板或公共資訊活動；

d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;
面對面之情境，例如回應民意調查或親自申請相關服務：口頭說明或以紙本或電子格式提供書面說明；

e. "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.
CCTV /無人機錄製之「即時」情境：顯示板包含之資訊、公共看板、公共資訊活動或報紙/媒體通知。

Information on profiling and automated decision-making
有關資料剖析和自動決策之資訊

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling[35] which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(F) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal

data, equally apply to profiling generally (not just profiling which is captured by Article 22[36]), as a type of processing.[37]

第22條第1項和第22條第4項所述之現存自動決策資訊（包括資料剖析）、與所涉邏輯相關之有意義資訊，及運用對當事人產生重大和預設之後果，皆構成依據第13條第2項第f款和14條第2項第g款中必須向當事人提供之強制資訊之一部分。WP29制定了關於自動化個人決策和資料剖析之指引[35]，針對特定資料剖析時如何實現透明化，應進一步參考這些指引。應注意的是，除依第13條第2項第f款和第14條第2項第g款規定之自動決策應適用的具體透明化要件外，這些指引中有關通知當事人運用其個人資料後果之重要性的評論，以及當事人不應就運用其個人資料而感到意外之一般原則，同樣普遍適用於資料剖析之情況（不僅限於第22條所涵蓋之剖析[36]），因其亦屬資料運用類型之一。[37]

Other issues – risks, rules and safeguards

其他議題 - 風險、規則和安全維護措施

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs,[38] data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

GDPR前言第39點亦提及某些第13條、第14條未明確涵蓋之應提供資訊（請參閱前文第28段前言文字）。該前言指出使當事人了解與個人資料運用相關之風險、規則和安全維護措施亦與其他議題有所關聯。其中包含個資保護影響評估（DPIAs）。如WP29關於DPIA之指引所述，[38] 資料控管者可考慮公佈DPIA（或其中一部分），作為促進對運用作業之

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

WP 251，第2016/679號規則，關於自動化個人決策和資料剖析指引，。

[36]This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.

此條款適用於僅基於自動化運用（包括剖析）對有關當事人產生法律效果或類似重大影響之決策。

[37] Recital 60, which is relevant here, states that "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".

前言第60點就此相關之部分指出，「此外，當事人應被告知資料剖析之存在以及該剖析之後果」。

[38] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a

信任，並做為展現透明化和課責性的一種方式，雖然此類公佈非屬強制性。此外，遵守行為守則（依據第40條之規定）可用於證明透明化，因行為守則可能就是以適用下列GDPR相關規範為目的所草擬：公正透明之運用；向公眾和當事人提供資訊；向兒童提供資訊以及保護等議題。

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

與透明化相關之另一議題為資料保護設計（by design）和預設（by default）（依據第25條之要求）。這些原則要求資料控管者從一開始便將資料保護考量納入其運用作業和系統，而非將資料保護視為最後的法遵議題。前言第78點指出資料控管者應執行符合設計及預設資料保護要求之措施，包含與個人資料之功能和運用相關之透明化措施。

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data controllers must be made available to the data subject. In other words, it must be completely clear to a data a subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR.[39]

此外，共同控管者的議題亦與使當事人知悉風險、規則和安全維護措施相關。第26條第1項要求共同控管者以透明之方式確認各自履行GDPR所定義務之責任，尤其是關於當事人行使其權利及依據第13條和第14條所需提供資訊之義務。第26條第2項要求資料控管者間之實質安排必須提供予當事人。易言之，若當事人欲行使其在GDPR下之一項或多項權利時，該當事人必須清楚知道應聯繫何資料控管者。[39]

Information related to further processing

與進階運用相關之資訊

---

high risk" for the purposes of Regulation 2016/679, WP 248 rev.1

WP 248 rev.1，第2016/679號規則有關個資保護影響評估（DPIA）指引和確認運用是否「可能造成高風險」。

[39] Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

依據第26條第3項，不論第26條第1項規定之共同資料控管者間之安排條件為何，當事人可依據GDPR對任一共同資料控管者行使其權利。

45. Both Articles 13 and Article 14 contain a provision[40] that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/ obtained. If so, *"the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2".* These provisions specifically give effect to the principle in Article 5.1(B) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is *incompatible* with these purposes is prohibited.[41] The second part of Article 5.1(B) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are *compatible* with the original purposes (Article 6.4 informs this issue[42]), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing for a particular purpose may take place.[43] In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

第13條和第14條皆規定[40]，若資料控管者欲進階運用個人資料之目的不同於蒐集/取得該資料之原始目的時，必須通知當事人。若為此情況，「*控管者在進階運用之前，應提供當事人有關該其他目的之資訊以及第2項所述之任何相關進階資訊*」。這些規定具體實現第5條第1項第b款規定，蒐集個人資料之目的應特定、明確及合法，且不得以*不符合*該等目的之方式做進階運用之原則。[41] 第5條第1項第b款第二部分規定，當進階運用係基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，則依第89條第1項規定，不應視為不符合原始目的。當進階運用個人資料*符合*原始目的時（第6條第4項說明此議題[42]），適用第13條第3項和第14條第4項之規定。這些條款規定向當事人提供有關進階運用資訊

[40] At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word "collected", which is used in Article 13, and which is replaced with the word "obtained" in Article 14.
第13條第3項和第14條第4項使用相同之術語表達，除第13條中使用「蒐集」一詞，而第14條中以「取得」一詞替代。

[41] See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89
該原則之示例請參閱前言第47、50、61、156、158點；第6條第4項和89條。

[42] Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.
第6條第4項以非完全列舉之方式規定在確認用於其他目的之運用是否與最初收蒐集個人資料之目的相符時所應考量之因素，即：目的間之關聯；蒐集個人資料之背景；個人資料之性質（尤其是特殊類型之個人資料或個人資料與刑事前科和犯罪相關聯時）；進階運用對當事人可能造成之後果；以及是否存在適當安全維護措施。

之要求，體現了在GDPR下當事人應得合理期待在蒐集個人資料時或過程中，皆係基於特定目的之運用。[43] 換言之，當事人不應就運用其個人資料之目的而感到意外。

46. Articles 13.3 and 14.4, insofar as they refer to the provision of *"any relevant further information as referred to in paragraph 2",* may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "*other necessary information*".) However the default position is that all such information set out in that sub-article should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

由於第13條第3項和14條第4項規定「*第2項所述之任何相關進階資訊*」，初看可解釋為該條款就第13條第2項或14條第2項第2款應提供予當事人之相關資訊的程度和特定種類，為控管者留有評估之空間。（前言第61點將此類資訊稱為「*其他必要資訊*」。）然而，預設之立場為該款所列之所有資訊，除有一種或多種資訊不存在或不適用之情形外，皆應提供予當事人。

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice on the compatibility analysis carried out under Article 6.4[44] where a legal basis other than consent or national/ EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others.[45] Where controllers choose not to include such information in a privacy notice/ statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

WP29建議，為符合透明、公正和課責義務，當新的運用目的之法律依據並非來自於同意或國家/歐盟法律，控管者應考量在其隱私聲明/通知中向當事人提供有關依據第6條第4項[44]所為之兼容性分析資訊。（換言之，關於其他運用目的與原始目的相容之解釋）。旨在使當事人有機會考量進階運用之兼容性和所提供之安全維護措施，並決定是否行使其權利，例如：限制運用之權利或拒絕運用之權利等。[45] 若控管者選擇不在隱私通知/

[43] Recitals 47 and 50
前言第47和50點。
[44] Also referenced in Recital 50
另參考前言第50點。
[45] As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and

聲明中提供此類資訊，WP29建議其向當事人明確表明可依據請求取得資訊。

48. Connected to the exercise of data subject rights is the issue of timing. As emphasised above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to *further processing* must be provided "prior to that further processing". WP29's position is that a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

與當事人權利行使相關者為時間點之問題。如上所述，及時提供資訊是第13條和第14條透明化要求下的一個重要條件，本質上並與公正運用之概念相關。與*進階運用*相關之資訊必須在「進階運用前」提供。WP29之立場為，在通知和開始運用間應存在合理期間，即不得在當事人收到通知後立即開始運用。此為透明化原則給予當事人之實質效益，使其有機會就進階運用做有意義的思考（並可能行使與進階運用相關之權利）。合理期間之範圍取決於具體情狀。公正性原則要求當進階運用越具侵害性（或較難預期），期間應越長。同樣，課責性原則要求資料控管者能夠證明，在該情境下提供該資訊的時間相關之決策於此種情狀下為合理的，以及整體時間之決策對當事人係公正的。（請另參閱上文第30至32段關於確認合理期間之意見。）

Visualisation tools

視覺化工具

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58[46] indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online

to verify the lawfulness of the processing.

如前言第63點所述，如此將使當事人得行使其近用權以了解並檢視運用之合法性。

environment.[47]

重要的是，GDPR下之透明化原則不僅限於透過語言溝通（書面或口頭）而實現。GDPR規定在適當情況下可提供視覺化之工具(特別是圖示、認證機制和資料保護標章和標誌)。前言第58點[46]指出，在網路環境中，向公眾或當事人傳達資訊的可得性尤為重要。[47]

Icons

圖示

50. Recital 60 makes provision for information to be provided to a data subject "in combination" with standardised icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:

前言第60點指出提供予當事人之資訊可與標準化圖示「組合」，從而允許多層次之方式。然而，圖示之使用不應替代當事人行使權利所必需之資訊，亦不應作為資料控管者符合第13條和第14條所定義務之替代。第12條第7項規定使用此類圖示之情況：

> "*The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable*".
>
> 「*依據第13條和第14條提供予當事人之資訊，可與標準化圖示組合使用，以便提供易見、易懂且清晰易讀之方式，並就預計之運用提出有意義之概述。當圖示係以電子方式呈現時，應使用機器可讀取之方式。*」

51. As Article 12.7 states that *"Where the icons are presented electronically, they shall be machine- readable",* this suggests that there may be situations where icons are not presented electronically,[48] for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.

如第12條第7項所述「*當圖示係以電子方式呈現時，應使用機器可讀取之方式*」，這表示可能存在圖示非以電子方式呈現之情況，[48]例如圖示標示於實體文書上、於物聯網設備

---

[46] "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."

「此類資訊可使用電子形式提供，例如當透過網站向公眾傳達資訊。尤其在行為者眾多且實務技術複雜之情形下，會造成當事人難以知悉並理解其個人資料是否、由誰、以何目的被蒐集，例如網路廣告之情形。」

[47] In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).

於此情形下，控管者應考量視覺受損之當事人（例如紅綠色盲）。

[48] There is no definition of "machine-readable" in the GDPR but Recital 21 of Directive 2013/37/EU17 defines "machine- readable" as:

GDPR中並無「機器可讀取」之定義，但第2013/37 / EU17號指令前言第21點將「機器可讀取」定義為：

或物聯網設備包裝上、公共場所關於Wi-Fi追蹤之通知上、於QR碼和CCTV之通知上。

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardisation of symbols/ images to be universally used and recognised across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons.[49] WP29 recognises that, in line with Recital 166, the development of a code of icons should be centered upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.

顯然地，使用圖示之目的在透過可能地減少向當事人呈現大量書面資訊之需要來增強對當事人之透明化。然而，圖示能否有效地將第13條和第14條所要求之資訊傳達予當事人，取決於該符號/圖像之標準化是否在歐盟境內被普遍使用和承認作為相關資訊之簡化圖示。有鑑於此，GDPR將制定圖示代碼之責任交予執委會，但最終歐洲個人資料保護委員會（EDPB）可應執委會之要求，或自行向執委會提供有關此類圖示之意見。[49] WP29認為，與前言第166點一致，圖示代碼之建立應以循證方式為中心，且為使圖示能有效之使用，於標準化之前，有必要與產業和廣泛大眾一起進行大規模之研究。

"a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats."

「一種文件格式，使軟體應用程式可輕鬆確認、識別和提取特定資料，包括各別事實陳述及其內部結構。以機器可讀取格式建立之文件中所編碼之資料屬於機器可讀取之資料。機器可讀取格式可以是開放或專有的；其可為正式或非正式之標準。若以限制自動運用文件格式編碼之文檔，因不得或不易從中提取資料，所以不應視為係機器可讀取之格式。成員國應酌情鼓勵使用開放、機器可讀取之格式。」

[49] Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

第12條第8項規定，執委會有權依據第92條委託，以確認圖示所呈現之資訊和提供標準化圖示之資訊。具有指導意義之前言第166點（有關執委會一般之委託行為）指出，執委會在籌備工作期間，必須進行包括專家層級之適當諮詢。然而，歐洲個人資料保護委員會（EDPB）在圖示標準化上也扮演重要的諮詢角色，因第70條第1項第r款規定，EDPB應主動或在相關的情況下應執委會要求，向執委會提供關於圖示之意見。

Certification mechanisms, seals and marks

認證機制、標章和標誌

53. Aside from the use of standardised icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects.[50] WP29 will be issuing guidelines on certification mechanisms in due course.

除使用標準化圖示外，GDPR（第42條）亦規定使用資料保護認證機制、資料保護標章和標誌，以證明資料控管者和受託運用者符合GDPR運用作業規範，並提高對當事人之透明化。[50] WP29將在適當時機公布認證機制指引。

Exercise of data subjects' rights

當事人權利之行使

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned, as they must:[51]

就GDPR下當事人之權利而言，透明化對資料控管者課予三重義務，因其必須：[51]

- provide information to data subjects on their rights[52] (as required under Articles 13.2(B) and 14.2(c));

  向當事人提供有關其權利之資訊[52]（依據第13條第2項第b款和14條第2項第c款之要求）；

- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and

  在與當事人就第15條至第22條和第34條下之權利進行溝通時需遵守透明化原則（即關於第12條第1項規定之溝通品質）；以及

- facilitate the exercise of data subjects' rights under Articles 15 to 22.

  促進第15至22條當事人權利之行使。

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to *meaningfully position* data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal

[50] See the reference in Recital 100

請參閱前言第100點。

[51] Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)

依據GDPR關於當事人權利之透明化和形式章節（第1節，第3章，即第12條）。

[52] Access, rectification, erasure, restriction on processing, object to processing, portability

近用、改正、刪除、限制運用、拒絕運用、可攜。

data. Recital 59 emphasises that *"modalities should be provided for facilitating the exercise of the data subject's rights"* and that the data controller should *"also provide means for requests to be made electronically, especially where personal data are processed by electronic means".* The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

GDPR關於當事人權利之行使和所需提供資訊之本質係為*有意義地定位*當事人，以使其維護自身權利並使資料控管者就其個人資料之運用負責。前言第59點強調「*應提供有利當事人行使其權利之形式*」，且資料控管者「*亦應提供以電子化請求之方式，特別是在透過電子方式運用個人資料時*」。資料控管者為當事人提供行使其權利之形式應符合控管者和當事人間之關聯和互動之本質。為此，資料控管者可能希望提供一種或多種不同行使權利之形式，以對應當事人與其各種互動方式。

Example
示例

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.

醫療衛生服務提供者為便於當事人以網路和當面申請個人資料之近用請求，在其網站上使用電子表格，而在診所服務台使用紙本表格。雖已提供這些型式，但醫療服務仍接受以其他方式（例如透過信件和電子郵件）申請近用請求，並提供專門的聯絡點（可透過電子郵件和電話連絡）以協助當事人行使其權利。

Exceptions to the obligation to provide information
提供資訊義務之例外情形

Article 13 exceptions
第13條之例外情形

56. The only exception to a data controller's Article 13 obligations where it has collected personal data directly from a data subject occurs *"where and insofar as, the data subject already has the*

information".[53] The principle of accountability requires that data controllers demonstrate (and document) what information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase "insofar as" in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

資料控管者第13條義務唯一例外情形為，當直接向當事人蒐集個人資料時，「*在該範圍內，當事人已擁有相關資訊*」[53]。課責性原則要求資料控管者證明（並記錄）當事人已擁有之資訊、取得該資訊之方式和時間以及未發生使該資訊過時之變更。此外，在第13條第4項中使用「就其範圍」一詞清楚表示，即使當事人先前已從第13條規定之資訊清單中取得某些類別之資訊，資料控管者仍有義務補充該資訊，以確保當事人擁有第13條第1項和13條第2項所列舉之完整資訊。以下為第13條第4項例外情形應被有限解釋之最佳實務示例。

Example
示例

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already has from 6 months ago and which has not since changed (e.g. the identity and contact details of the controller and the data protection officer, information on data subject rights and the right to complain to the relevant supervisory authority). As a matter of best practice however, the complete suite of information should be provided to the data subject again but the data subject also should be able to easily tell what information amongst it is new. The new processing for the purposes of the instant messaging service may affect the data subject in a way which would prompt them to seek to exercise a right they may have forgotten about, having been informed six months prior. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and their rights.

[53] Article 13.4
第13條第4項。

某當事人註冊網路電子郵件服務，並在註冊時收到第13條第1項和13條第2項規定之所有必要資訊。六個月後，該當事人透過電子郵件服務提供者啟用連結即時訊息功能，並提供其手機號碼。服務提供者向當事人提供依據第13條第1項和13條第2項關於手機號碼運用之資訊（例如運用之目的和法律依據、接收者、保存期限），但未提供當事人於六個月前已獲得且無變更之資訊。（例如控管者和個資保護長之身分和聯絡方式，有關當事人權利之資訊以及向相關監管機關申訴之權利）。然而，最佳實務做法是，應再次向當事人提供整套完整之資訊，但亦應能使當事人輕易辨別其中最新之資訊。此即時訊息服務之新運用行為，可能會促使當事人行使其在六個月前被告知卻可能遺忘之權利。再次提供所有資訊有助於確保當事人充分瞭解其資料被使用之方式和其權利。

Article 14 exceptions

第14條之例外情形

57. Article 14 carves out a much broader set of exceptions to the information obligation on a data controller where personal data has not been obtained from the data subject. These exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the circumstances where the data subject already has the information in question (Article 14.5(A)), Article 14.5 also allows for the following exceptions:

當個人資料並非從當事人取得時，第14條規定了資料控管者提供資訊義務更廣泛之例外情形。作為一般法律規則，這些例外應被狹義地解釋和適用。除當事人已取得相關資訊之情狀（第14條第5項第a款）外，第14條第5項亦允許以下例外情形

- The provision of such information is impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or where it would make the achievement of the objectives of the processing impossible or seriously impair them;

  提供此類資訊係不可能，或不成比例之付出，特別是基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，或其可能造成無法實現運用目的或嚴重損害該目的；

- The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests ; or

  資料控管者取得或揭露個人資料依據成員國法律或歐盟法律之要求，且該法律為當事人之合法利益提供適當之保護；或

- An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential.

依據成員國或歐盟法律規定之職業保密義務（包括法定之保密義務），即個人資料必須保密。

Proves impossible, disproportionate effort and serious impairment of objectives
證明為不可能、不符合比例原則和嚴重損害目的

58. Article 14.5(B) allows for 3 separate situations where the obligation to provide the information set out in Articles 14.1, 14.2 and 14.4 is lifted:
第14條第5項第b款條允許第14條第1項、14條第2項和14條第4項規定所應提供資訊義務之三種各別例外情形：

(i) Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
當提供資訊被證明係不可能之情形（尤其是基於為歸檔、科學/歷史研究或統計之目的）;

(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/ historical research or statistical purposes); or
當提供資訊為不成比例之付出（尤其是基於歸檔、科學/歷史研究或統計之目的）；或

(iii) Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.
當提供第14條第1項要求之資訊將無法實現運用之目的或嚴重損害該目的。

"Proves impossible"
「證明為不可能」

59. The situation where it "proves impossible" under Article 14.5(B) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually *prevent it* from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.
第14條第5項第b款中所謂當提供資訊被「證明為不可能」之情形應屬一種可提供全部資訊或完全無法提供資訊之情形，因為不可能是沒有程度上之區分。因此，若資料控管者試圖援用此類例外情形，則必須證明有實際上*阻止其*向當事人提供有關資訊之因素。若在一段期間後，導致「不可能性」之因素已不存在，且可向當事人提供資訊時，資料控管者應立即為之。實際上，僅在少數情況下資料控管者可證明其事實上不可能向當事人

提供資訊。請參閱以下示例。

Example
示例

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller's protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject's address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.

當事人註冊一項後付費線上訂閱服務。註冊後，資料控管者從聯合徵信機構蒐集有關當事人之信用資料，以決定是否提供服務。依據第14條第3項第a款，控管者應在蒐集該信用資料後之三天內通知當事人。然而，當事人之地址和電話號碼並未註冊於公共註冊管理機構（當事人實際上居住於國外）。註冊服務時當事人未留下電子郵件地址或電子郵件地址無效。控管者發現無法直接聯繫當事人。然而，在此情況下，控管者可在註冊之前於其網站上提供關於徵信資料蒐集之資訊。在此情況下，提供第14條規定之資訊並非不可能。

Impossibility of providing the source of the data
無法提供資料來源

60. Recital 61 states that "where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided". The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by

design and by default,[54] transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).

前言第61點指出「因使用了各項資料來源，而無法向當事人提供個人資料來源時，應提供一般資訊」。免除向當事人提供關於其個人資料來源資訊之要求，僅適用於因與同一當事人相關之各種個人資料無法追溯至特定來源，而無法提供之情況。例如，資料控管者使用多種來源將多位當事人之個人資料彙集成數據庫，若控管者能夠（雖然耗時或費力）確認個別當事人之個人資料來源，則此一事實尚不足以免除該項要求。有鑑於資料保護設計（by design）和預設（by default）之要求[54]，透明化機制應從底層開始構建至運用系統中，以便組織接收到的所有個人資料皆可在運用過程中的任一時點追蹤和追溯至其來源。（請參閱上文第43段）。

"Disproportionate effort"

「不成比例之付出」

61. Under Article 14.5(B), as with the "proves impossible" situation, "disproportionate effort" may also apply, in particular, for processing *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)".* Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29's position is that this exception should not be *routinely* relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

依據第14條第5項第b款，與「證明為不可能」之情況相同，「不成比例之付出」亦可適用，特別是當運用係「*基於公共利益之歸檔目的、科學或歷史研究目的或統計目的，且符合第89條第1項之安全維護措施*」。前言第62點亦將這些目的作為向當事人提供資訊不成比例之付出的案例，並指出，應考量當事人之數量、資料之年代和所採行之任何適當安全維護措施。有鑑於前言第62點和第14條第5項第b款強調關於適用此項豁免之歸檔、

[54] Article 25
第25條。

研究和統計目的，WP29之立場為，若資料控管者運用資料之目的並非為了公共利益之歸檔目的、為了科學或歷史研究目的或統計目的，該控管者不應*經常性地*援用此例外情形。WP29強調，即使為這些目的而運用，仍須遵守第89條第1項規定之要件，且提供資訊應達到不成比例之付出。

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(B), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.

在考量如何構成第14條第5項第b款之「不可能」或「不成比例之付出」時，第13條（從當事人蒐集個人資料）之情形並無與此相當之豁免。第13條和第14條唯一的區別在於，後者之個人資料並非從當事人處蒐集。因此，「不可能」或「不成比例之付出」在通常情況下不適用於從當事人蒐集個人資料之情形。換言之，「不可能」或「不成比例之付出」必須與個人資料並非從當事人取得之事實有直接關聯。

Example
示例

A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.

一家綜合醫院要求所有進行日間手術、長期住院和預約之病患填寫病患資料表格，該表格要求填寫兩位近親（當事人）之詳細資訊。由於每天出入醫院病人之數量非常龐大，若要求醫院提供第14條中之資訊給每日被病患在表格上列為近親之所有當事人，對醫院構成不成比例之付出。

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14 information.

前言第62點中提及之因素（當事人之數量、資料之年代和所採行之任何適當安全維護措施）指明某些類型情況可能導致資料控管者必須以不成比例之付出通知當事人第14條相關資訊。

Example
示例

Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50 years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

歷史研究人員為透過姓氏追溯血緣，間接獲得了與20,000個當事人相關之大型資料集。然而，該資料集係蒐集於50年前，且自此後並無更新，亦不包含任何聯絡方式。鑑於資料集之規模，特別是資料之年代，要求研究人員試著逐一追踪當事人以向其提供第14條之資訊屬不成比例之付出。

64. Where a data controller seeks to rely on the exception in Article 14.5(B) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(B) specifies that the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(B), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimising the data collected and the storage period; and implementing technical and organisational measures to ensure a high level of security. Furthermore, there may be

situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

當資料控管者因提供資訊將不符合比例原則而欲援用第14條第5項第b款之例外情形時，該控管者應該進行平衡判斷，評估提供資訊所涉及之工作量，以及若未提供該資訊予當事人將對其產生之影響和結果。資料控管者應依據其課責性義務記錄此評估。在此情況下，第14條第5項第b款規定，控管者必須採取適當措施保護當事人之權利、自由和合法利益。此原則亦適用於當控管者確認資訊之提供為不可能時，或可能導致運用目的無法實現或嚴重損害該目的之達成。依據第14條第5項第b款之規定，控管者必須採行的一項適當措施為公開資訊。控管者可透過多種方式達到此目的，例如將資訊放置於網站上、或主動在報紙上宣傳該資訊或在其場所張貼相關資訊海報。除了公開資訊外，其他適當措施將取決於運用之具體情狀，但可包含：踐行個資保護影響評估；使用資料假名化技術；資料蒐集和儲存期之最小化；以及實施技術性和組織性之措施，以確保高度安全保護。此外，資料控管者正在運用的個人資料亦可能不需識別當事人（例如，使用假名化資料）。在此情況下，應考量第11條第1項，該條款規定若僅係為符合GDPR之規範，資料控者並無義務維護、取得或運用其他資訊以識別當事人。

Serious impairment of objectives

對目的之嚴重損害

65. The final situation covered by Article 14.5(B) is where a data controller's provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(B) pre-supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis.

第14條第5項第b款涵蓋之最後情況為，資料控管者依據第14條第1項向當事人提供資訊可能導致無法達成或嚴重損害該運用目的。欲援用此例外情形，資料控管者必須證明僅提供第14條第1項規定之資訊將使運用之目的無效。另須注意，援用第14條第5項第b款須預先假定資料運用符合第5條規定之所有原則，最為重要者，在所有情狀下，個人資料之運用係公正的，並有法律依據。

Example
示例

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to "tip off" the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(B) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder's personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of "tip-offs". However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

A銀行為遵守反洗錢法規之強制性要求,必須向相關金融執法機關通報與其持有帳戶有關之可疑活動。A銀行從B銀行（另一個成員國）收到一則資訊，即某帳戶持有人指示B銀行轉賬到A銀行一個看似可疑之賬戶。A銀行將有關其賬戶持有人和可疑活動之資料傳送給相關金融執法機關。相關反洗錢法規規定，若通報銀行「密報」帳戶持有人其可能受到監管調查，則屬於刑事犯罪。此情況適用第14條第5項第b款，因向當事人（A銀行賬戶持有人）提供第14條有關運用從B銀行接收之賬戶持有人個人資料之資訊，將嚴重損害法規之目的，包含妨礙「密報」。然而，在開立賬戶時，A銀行應向所有賬戶持有人提供一般性資訊，告知其個人資料可能運用於反洗錢目的。

Obtaining or disclosing is expressly laid down in law
法律明文規定之取得或揭露

66. Article 14.5(C) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data *"is expressly laid down by Union or Member State law to which the controller is subject"*. This exemption is conditional upon the law in question providing *"appropriate measures to protect the data subject's legitimate interests"*. Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either

obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides "*appropriate measures to protect the data subject's legitimate interests"*, the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data *directly from a data subject*, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.

若取得或揭露個人資料係「*依據控管者所受拘束之歐盟法律或成員國法律明文規定*」，第14條第5項第c款允許第14條第1項、第2項和第4項所要求提供資訊之免除。此項例外情形是以相關法律須提供「*保護當事人合法利益之適當措施*」為要件。該法律必須直接規範資料控管者，且取得或揭露對資料控管者而言應為強制性。因此，資料控管者必須能證明相關法律之適用，以及該法律如何要求其取得或揭露相關個人資料。雖然歐盟或成員國法律須建構以提供「*保護當事人合法利益之適當措施*」，但資料控管者應確保（並能夠證明）其取得或揭露個人資料係符合此類措施。 此外，除非法律明文禁止，資料控管者應向當事人具體說明其取得或揭露個人資料係根據相關法律規定。此亦符合GDPR前言第41點，該前言指出，依據歐盟法院和歐洲人權法院案例法，法律依據或立法措施應當清楚和明確，且受其拘束之個人應可預見該法律之適用。然而，若資料控管者有義務*直接從當事人取得資料*，在此情況下，適用第13條而不適用第14條第5項第c款。在該情況下，GDPR中唯一得免除控管者向當事人提供相關運用資訊者為第13條第4項之規定（即在該範圍內，當事人已擁有相關資訊）。然而，如下文第68段所述，在國家層級，成員國亦可依據第23條立法，對第12條規定之透明化和第13條和第14條規定之資訊做出進一步具體限制。

Example

示例

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.

稅務機關必須遵守國家法律強制性之要求，從雇主取得員工薪資詳情。該個人資料並非從當事人取得，因此稅務機關必須符合第14條之要求。由於稅務機關從雇主取得個人資料係法律所明文規定，因此第14條對資訊之要求於此情況下不適用於該稅務機關。

Confidentiality by virtue of a secrecy obligation

保密義務下之機密性

67. Article 14.5(D) provides for an exemption to the information requirement upon data controllers where the personal data "*must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy*". Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

第14條第5項第d款規定，當個人資料「*依據歐盟或成員國法律所定專業保密義務之規範(包括法定之保密義務)，應予保密*」時，可免除對資料控管者提供資訊之要求。若資料控管者欲援用此例外規定，必須能夠證明其已適當確認此類例外，且說明專業保密義務如何直接規範資料控管者，以禁止資料控管者向當事人提供所有第14條第1項、第2項和第4項規定之資訊。

Example

示例

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(D) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

醫生（資料控管者）對其病患的醫療資訊負有專業保密義務。病患（適用於專業保密義務者）向醫生提供有關其遺傳情況的健康資訊，該遺傳情況亦發生在病患的某些近親身上。病患還向醫生提供具有相同症狀親屬（當事人）的某些個人資料。基於第14條第5項第d款之豁免，醫生無需向這些親屬提供第14條之資訊。若醫生向親屬提供第14條之資訊，則違反其對病患之專業保密義務。

Restrictions on data subject rights

當事人權利之限制

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights[55] where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(A) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such *a national legislative restriction* to the exercise of data subject

rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/ 2017[56] that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

第23條規定成員國（或歐盟）得在尊重基本權利和自由之本質，並為保障第23條第1項第a至j款10項目的中之一項或多項之必要且符合比例原則時，就與當事人權利範圍相關之透明化和實質當事人權利[55]為進一步限制。若此類國家措施減少特定當事人權利，或依GDPR應適用於資料控管者之一般透明化義務時，資料控管者應能夠證明國家法規如何適用。如第23條第2項第h款所述，除非有損害限制目的之虞，否則立法措施必須包含當事人有權被告知其權利受到限制之規定。同樣地，基於公正原則，除非有損立法限制目的之虞，否則資料控管者亦應告知當事人行使權利或透明化義務之限制所依據（或在當事人行使特定權利時將依據）之*國家法律為何*。因此，透明化要求資料控管者向當事人提供與其權利相關之所有資訊，以及控管者對該權利得以採行之任何特別中止情事，使當事人嗣後試圖對控管者行使其特定權利時，不至因可能之限制而感到意外。就假名化和資料最小化，以及資料控管者可能援用之GDPR第11條而言，WP29先前已在第3/2017[56]號意見中確認，GDPR第11條應被解釋為在不妨礙當事人權利行使之情況下，執行實質資料最小化的一種方式，且必須藉由當事人提供其他資訊以實現當事人權利之行使。

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.

[55] As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.
如第12條至第22條和第34條以及第5條所述，該條款須與第12條至第22條規定之權利和義務相對應。

[56] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2
第03/2017號意見關於在合作智能運輸系統（C-ITS）之個人資料運用 - 請參閱第4.2段。

此外，第85條要求成員國依法調和資料保護與言論及資訊自由權。除其他事項外，成員國因新聞、學術、藝術或文學言論目的之運用，而有必要調和此二項權利時，得就GDPR某些條款之適用予以適當的豁免或免除（包括第12-14條之透明化要求）。

Transparency and data breaches

透明化和個資侵害

70. WP29 has produced separate Guidelines on Data Breaches[57] but for the purposes of these guidelines, a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12.[58] The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

WP29另制定了個資侵害指引[57]，但就本指引而言，資料控管者關於與當事人就個資侵害進行溝通之義務，必須充分考量第12條[58]規定之透明化要求。就個資侵害之溝通必須符合前文所述之相同要件（尤其是使用明確和簡明之語言），這些要件於與當事人就其權利或就第13條和第14條所須提供之資訊進行溝通時亦適用之。

[57] Guidelines on Personal data breach notification under Regulation 2016/679, WP 250
WP250，關於第2016/679號規則(GDPR)中的個人資料侵害通知之指引。

[58] This is made clear by Article 12.1 which specifically refers to "…any communication under Articles 15 to 22 **and 34** relating to processing to the data subject..." [emphasis added].
第12條第1項明確規定並具體提及「...依據第15條至第22條**和第34條**所定關於對當事人所為運用之任何溝通...」[重點強調]。

Annex

Information that must be provided to a data subject under Article 13 or Article 14

Required Information Type	Relevant article (if personal data collected directly from data subject)	Relevant article (if personal data not collected directly from data subject)	WP29 comments on information requirement
The identity and contact details of the controller and where application, their representatives[59]	Article 13.1(a)	Article 14.1(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc)
Contact details for the data protection officer, where applicable	Article 13.1(b)	Article 14.1(b)	See WP29 Guidelines on Data Protection Officers[60]
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.1(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.
Where legitimate interests (Article 6.1(F)) is the legal basis for the processing, the legitimate interests pursued by the data controllers or third party	Article 13.1(d)	Article 14.2(b)	The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the balancing test, which must be carried out to allow reliance on Article 6.1(F) as a lawful basis for processing, in

			advance of any collection of data subject's personal data. To avoid information fatigue, this can be included within a layered privacy statement /notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.
Categories of personal data concerned	Not required	Article 14.1(d)	This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained.
Recipients[61] (or categories of recipients) of the personal data	Article 13.1(e)	Article 14.1(e)	The term "recipient" is defined in Article 4.9 as *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed,* ***whether a third party or not****" [emphasis added].* As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will

			generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.
Details of transfers to third countries, the fact of same and the details of the relevant safeguards[62] (including the existence or absence of a Commission adequacy decision[63]) and the means to obtain a copy of them or where they have been made available	Article 13.1(f)	Article 14.1(f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45/binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.
The storage period (or if not possible, criteria used to determine that period)	Article 13.2(A)	Article 14.2(a)	This is linked to the data minimization requirement in Article 5.1(C) and storage limitation requirement in Article 5.1(E). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for

			the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purpose, including where appropriate, archiving periods.
The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing and • portability.	Article 13.2(B)	Article 14.2(c)	This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.[64] In relation to the right to portability, see WP29 Guidelines on the right to data portability.[65]
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	Article 13.2(C)	Article 14.2(d)	This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.[66]
The right to lodge a complaint with a supervisory authority	Article 13.2(D)	Article 14.2(e)	This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.	Article 13.2(E)	Not required	For example in an employment context, it may be a contractual requirement to provide certain information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the

			required fields.
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source	Not required	Article 14.2(f)	The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/ privately held sources) and the types of organisation/ industry/ sector.
The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the fata subject	Article 13.2(F)	Article 14.2(g)	See WP29 Guidelines on automated individual decision -making and Profiling.[67]

附錄

依據第13條或第14條必須提供予當事人之資訊

所需資訊類型	相關條款（若直接從當事人蒐集個人資料）	相關條款（若並非直接從當事人蒐集個人資料）	WP29對資訊要求之意見
控管者之身分和聯絡方式，及其代表[59]（如適用）	第13條第1項第a款	第14條第1項第a款	此類資訊應可輕易辨別控管者，且可與資料控管者進行不同形式之溝通（例如電話號碼，電子郵件，郵政地址等）。
個資保護長之聯絡方式（如適用）	第13條第1項第b款	第14條第1項第b款	請參閱WP29個資保護長指引[60]
運用目的和法律依據	第13條第1項第c款	第14條第1項第c款	除表明運用個人資料之目的外，依第6條規定之相關法律依據亦須具體指明。對於特種個人資料，應當具體指明第9條之相關規定（及運用該資料應適用之相關歐盟或成員國法律）。依據第10條，涉及刑事前科與犯罪或第6條第1項相關安全措施之個人資料運用，若適用相關歐盟或成員國法律，亦應具體指明。
當運用之法律依據為資料控管者或第三人追求之合法利益（第6條第1項第f款）	第13條第1項第d款	第14條第2項第b款	為確保當事人之權益，必須說明具體相關利益。於蒐集任何當事人之個人資料前，必須依據第6條第1項F款辦理平衡判斷，作為運用之合法依據，而作為最佳實務，控管者亦可向當事人提供平衡判斷之資訊。

[59] As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the WU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behavior of, data subjects in the EU.

依據GDPR第4條第17款（並參考前言第80點）中之定義，「代表」係指設立於歐盟境內之自然人或法人，由控管者或受託運用者依據第27條以書面形式指定，並代表控管者或受託運用者履行GDPR下各自之義務。依據第3條第2項，該義務適用於當控管者或受託運用者非設立於歐盟境內，但運用位於歐盟境內當事人之個人資料，且該運用涉及對歐盟境內當事人提供商品或服務或監控其行為。

[60] Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017.

WP243 rev.01，個資保護長指引，於2017年4月5日最終修訂並通過。

			為避免資訊疲勞，可將其包含在分層隱私聲明/通知中（請參閱第35段）。無論如何，WP29之立場為，提供予當事人之資訊應明確表明可依據要求取得有關平衡判斷之資訊。這對於有效之透明化極為重要，尤其是當事人對平衡判斷之測試執行是否公正有疑慮，或希望向監管機關提請申訴時。
相關個人資料類型	無相關規定	第14條第1項第d款	第14條要求提供此類資訊，由於個人資料並非從當事人取得，因此當事人無法知悉資料控管者取得何種類型之個人資料。
個人資料接收者[61]（或接收者類型）	第13條第1項第e款	第14條第1項第e款	第4條第9款將「接收者」一詞定義為「*向其揭露個人資料之自然人或法人、公務機關、局處或其他機構，**不論其是否為第三方***」[*重點強調*]。所以，接收者不需為第三方。因此，「接收者」一詞涵蓋了向其傳送或揭露資料之其他資料控管者、共同控管者和受託運用者。且除了有關第三方接收者之資訊外，亦應提供有關此類接收者之資訊。 必須提供個人資料實際（指明）接收者或接收者之類型。基於公正原則，控管者必須提供對當事人最有意義的接收者資訊。實際上，此通常為指名接收者，以便當事人確切知道誰擁有其個人資料。若控管者選擇提供接收者類型，則資訊亦應透過表明接收者之類型（即參考其執行之活動）、行業、部門和子部門以及接收者的所在位置等方式，盡可能具體指明。
移轉至第三國之詳細資訊、相同維護措施之事實及	第13條第1項第f款	第14條第1項第f款	GDPR相關條文規定需具體表明資料之移轉和對應機制（例如，第45條的適足性認定/ 第47條的有拘束力之企業守則/ 第46

[61] As defined by Article 4.9 of the GDPR and referenced in Recital 31
依GDPR第4條第9款定義，並參考前言第31點。

相關維護措施[62]之詳細資訊（包括執委會是否做出適足性之決定[63]）、以及取得這些維護措施副本之方式或可於何處取得			條第2項的標準資料保護條款/ 第49條的例外和安全維護措施等）。亦應提供造訪或取得相關文件地點和方式之資訊，例如：透過提供所用機制之網址連結。基於公正原則，向第三國移轉資訊之提供應盡可能對當事人是有意義的；此通常意味著指明第三國國家。
儲存期限（若不可行，則為決定該期限之標準）	第13條第2項第a款	第14條第2項第a款	此與第5條第1項第c款中資料最少化要求和第5條第1項第e款中儲存限制要求相關。儲存期限（或決定期限之標準）可能由法定要求或行業指引等因素決定，但應允許當事人依據其自身情況評估對特定資料/目的之保留期限為何。若資料控管者的一般聲明為只要就運用之合法目的為必要，資料將盡可能長時間的被保留，則該聲明是不足夠的。在相關情況下，應針對不同類型之個人資料和/或不同運用目的規定不同之儲存期限。（包括適當歸檔期限）
當事人基於其權利得： • 近用 • 改正 • 刪除 • 限制運用 • 拒絕運用 • 可攜	第13條第2項第b款	第14條第2項第c款	此資訊應特定於運用情景，並提供概括資訊，包含所涉及之權利、當事人行使其權利之步驟以及對該權利之任何限制（請參閱前文第68段）。 尤其是，最遲在與當事人進行第一次溝通時，必須明確地使當事人注意到其拒絕運用之權利，且必須與任何其他資訊清楚地分開提供。[64] 關於可攜性，請參閱WP29資料可攜權之指引。[65]

[62] As set out in Article 46.2 and 46.3
如第46條第2項和46條第3項所述。
[63] In accordance with Article 45
依據第45條。
[64] Article 21.4 and Recital 70 (which applies in the case of direct marketing)
第21條第4項和前言第70點（適用於行銷案例）。
[65] Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017
WP 242 rev.01，資料可攜權指引，於2017年4月5日最終修訂並通過。

基於同意（或明確同意）所為之運用，有權隨時撤回同意	第13條第2項第c款	第14條第2項第d款	此資訊應包含如何撤回同意，同時考量到撤回同意應和給予同意一樣容易。[66]
向監管機關提出申訴之權利	第13條第2項第d款	第14條第2項第e款	此資訊應說明，依據第77條，當事人有權向監管機關提出申訴，特別是在其慣常居住地、工作地點或被指控違反GDPR之地點。
是否有法定或契約要求提供資訊，或是否有必要簽訂契約，或者是否有義務提供資訊以及未提供資訊可能之後果	第13條第2項第e款	無相關規定	例如，在工作環境中，契約可能要求提供某些資訊予目前或未來雇主。 網路表格應清楚表明哪些資訊是「必需的」，哪些不是，以及未填寫必填資訊之後果。
個人資料原始來源，如適用，是否來自可公開造訪之來源	無相關規定	第14條第2項第f款	除非無可能性，否則應提供具體資料來源—進一步指導請參閱第60段。若無法指名特定來源，則提供之資訊應包括：資料來源之性質（即公開/私人來源）和組織/行業/部門之類型。
自動化決策之存在，包括剖析和（如適用）與運用邏輯相關之有意義的資訊以及此類運用對當事人之重要性和預設之後果。	第13條第2項第f款	第14條第2項第g款	請參閱WP29關於自動化個人決策和剖析指引。[67]

[66] Article 7.3
第7條第3項。
[67] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
WP 251，關於第2016/679號規則(GDPR)中的自動化個人決策和剖析之指引。

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

17/EN

WP 248 rev.01

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

關於第2016/679號規則(GDPR)中的個資保護影響評估（DPIA）以及確認運用是否「可能造成高風險」之指引

Adopted on 4 April 2017

2017年4月4日通過

As last Revised and Adopted on 4 October 2017

2017年10月4日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及第2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

由歐盟執委會司法總署第C署（基本權利和歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 03/075號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing譯為「運用」，processor 譯為「受託運用者」。

Table of Content 目錄

I. Introduction
導言

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA[2]), as does Directive 2016/680[3].

第2016/679[1]號規則（GDPR）將自2018年5月25日起施行。GDPR第35條導入了個資保護影響評估（DPIA[2]）之概念，如同第2016/680[3]號指令。

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance**.

DPIA是一種描述資料運用、評估運用之必要性及合比例性的程序，並透過評估及決定因應措施，協助控管者管理因運用個人資料[4]而對自然人權利和自由產生之風險。DPIA

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2016年4月27日歐洲議會和歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，制定第2016/679號規則（EU），並廢除第95/46/EC號指令（一般資料保護規則）。

[2] The term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.
於其他情形常使用之「隱私影響評估」（PIA）一詞概念相同。

[3] Article 27 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, also states that a privacy impact assessment is needed for "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*".
2016年4月27日歐洲議會和歐盟理事會第2016/680號指令（EU）第27條關於權責機關為預防、調查、偵查或起訴刑事犯罪或執行刑事處罰而運用個人資料時，對自然人之保護與確保該資料之自由流通，亦指出若「*運用可能會對自然人之權利和自由造成高風險*」時，需進行隱私影響評估。

[4] The GDPR does not formally define the concept of a DPIA as such, but
GDPR並未正式定義DPIA本身之概念，然而

- its minimal content is specified by Article 35(7) as follows:
  依第35條第7項規定，其至少應包含以下內容：
  - "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
    「對預計運用作業和運用目的之系統性描述，於適用情形下，包含控管者尋求之合法利益；
  - *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes*
    與運用目的相關運用作業之必要性及合比例性之評估；
  - *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph*

是課責性的重要工具，因DPIA不僅可協助控管者遵守GDPR之要求，亦可使控管者證明已採取適當措施確保遵守本規則（請另參閱第24條）[5]。換言之，**DPIA是建立及證明合規性之程序**。

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever ishigher.

依據GDPR，不遵守DPIA之要求可能被權責監管機關處以罰鍰。當運用須辦理DPIA（第35條第1項和第3-4項）卻未辦理、未以正確方式辦理DPIA（第35條第2項和第7-9項）、或未依規定諮詢權責監管機關（第36條第3項第e款）時，可能被處以高達1千萬歐元之行政罰鍰，或於企業之情況下，最高可處前一會計年度全球年營業額之百分之二，以金額較高者為準。

II. Scope of the Guidelines
指引之範圍

These Guidelines take account of:

本指引依據：

1;and

第1項所述當事人權利和自由風險之評估；以及

- *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*

為因應風險而預計採行之措施，包含安全維護、安全措施和機制，以確保個人資料之保護，並在考量到當事人和其他相關人員之權利和合法利益之情況下證明對本規則之遵守」；

- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk"*

前言第84點已釐清其意義和角色如下：「為強化本規則之遵循，*當運用作業可能會對自然人之權利和自由造成高風險時，控管者應負責辦理個資保護影響評估，以檢視（尤其是）該風險之起源、性質、特殊性和嚴重性。*」

[5] See also recital 84: "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

請另參閱前言第84點：「*為證明個人資料之運用符合本規則，在決定應採行之適當措施時，評估結果應納入考量*」。

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP218[6];
  第29條個人資料保護工作小組（WP29）聲明，14/EN WP 218[6]；
- the WP29 Guidelines on Data Protection Officer 16/EN WP243[7];
  WP29個資保護長指引，16/EN WP 243[7]；
- the WP29 Opinion on Purpose limitation 13/EN WP203[8];
  WP29關於目的限制之意見，13 / EN WP 203[8]；
- international standards[9].
  國際標準[9]。

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by Data Protection Authorities (DPAs) under Article 35(4).
與體現於GDPR中之以風險為基礎的方法相符，DPIA並非對每個運用作業皆為強制性的。DPIA僅適用於當運用「*可能對自然人之權利和自由造成高風險*」時（第35條第1項）。為確保對強制辦理DPIA之情形作出一致解釋（第35條第3項），本指引首要目的即在於澄清此一概念，並為資料保護機關（DPAs）依據第35條第4項所應制定並公布須辦理DPIA的運用個資行為之清單提供標準。

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to

---

[6]WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532
14/EN WP 218，WP29於2014年5月30日通過關於資料保護法律架構下以風險為基礎的方法之作用聲明。
[7]WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A
16/EN WP 243，WP29於2016年12月13日通過關於個資保護長指引。
[8]WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409
13/EN WP 203，WP29於2013年4月2日通過第03/2013號關於目的之限制意見。
[9]e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).
例如 ISO 31000：2009，*風險管理 - 原則和指引*，國際標準化組織（ISO）; ISO / IEC 29134（項目），*資訊科技 - 安全技術 - 隱私影響評估 – 指引*，國際標準化組織（ISO）。

issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.

依據第70條第1項第e款，為鼓勵GDPR適用之一致性，歐洲個人資料保護委員會（EDPB）得發布指引、建議和最佳實務作法。本文件之目的係為EDPB未來之工作預先準備，從而澄清GDPR的相關規定，以協助控管者遵守法律，並為需要辦理DPIA之控管者提供法律確定性。

These Guidelines also seek to promote the development of:

本指引亦旨在促進下列事項之發展：

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
  歐盟通用之強制進行DPIA之運用作業清單（第35條第4項）；
- a common EU list of processing operations for which a DPIA is not necessary (Article35(5));
  歐盟通用之無需進行DPIA之運用作業清單（第35條第5項）；
- common criteria on the methodology for carrying out a DPIA (Article35(5));
  DPIA辦理方法之通用標準（第35條第5項）；
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
  具體指明何時應諮詢監管機關之通用標準（第36條第1項）；
- recommendations, where possible, building on the experience gained in EU Member States.
  在可能之情況下，借鑒歐盟成員國經驗做出之建議。

III. DPIA: the Regulation explained
DPIA：條文說明

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks[10] presented by the processing of personal data.

GDPR要求控管者採取適當措施以確保並能證明遵守GDPR，同時考量到「對自然人權利和自由造成各種可能和嚴重之風險」（第24條第1項）。控管者在某些情形下須辦理DPIA之義務應從其須適當管理個人資料運用風險[10]之一般義務的角度來理解。

A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.
「風險」是描述依據嚴重性和可能性進行估算的事件及其後果之可能情境。另一方面，「風險管理」可被定義為指導和控制組織中與風險相關之協調活動。

Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.
第35條係指「對個人之權利和自由」可能存在高風險之情況。如第29條個資保護工作小組關於風險基礎方法在資料保護法律架構中之作用的聲明所述，當事人之「權利和自由」主要考量的是資料保護和隱私之權利，然亦可能涉及其他基本權利，如言論自由、思想自由、行動自由、禁止歧視以及自由、良心和宗教之權利。

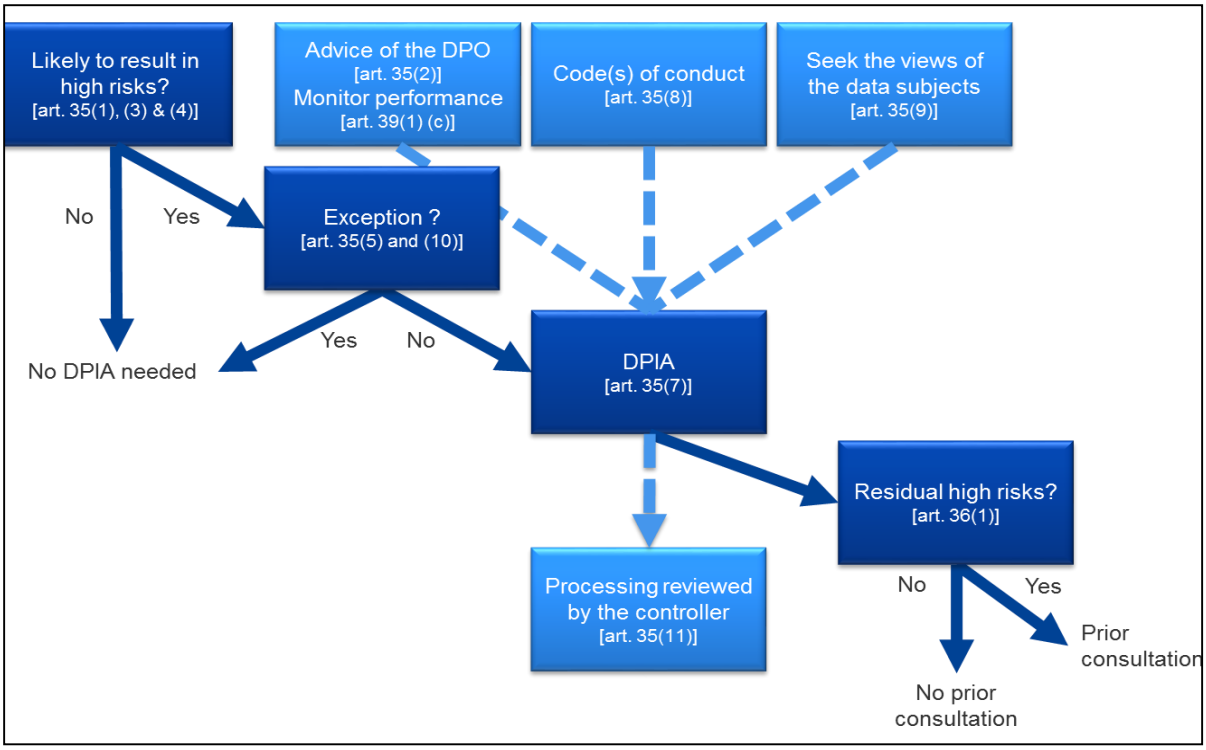
In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".
與體現於GDPR的風險基礎方法相符，DPIA並非對每個運用作業皆為強制性的。相反的，僅有當運用「可能對自然人之權利和自由造成高風險」時才需要DPIA（第35條第

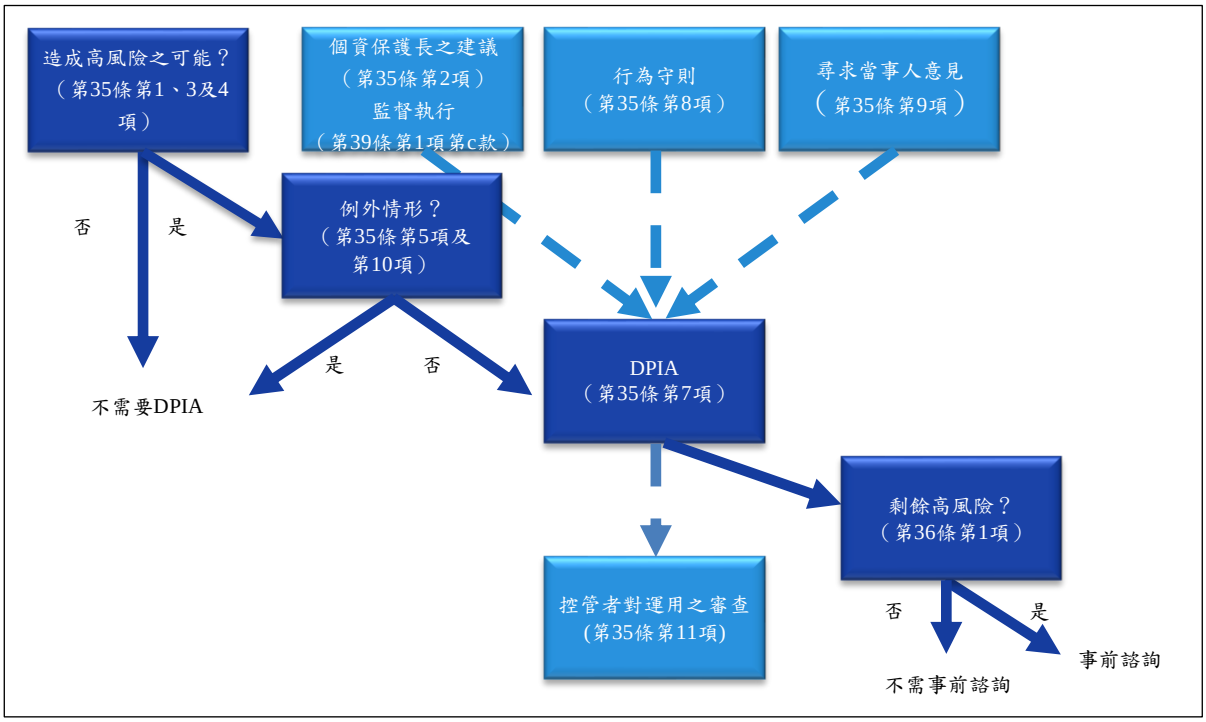
[10] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.
必須強調的是，為了管理自然人權利和自由之風險，必須辨識、分析、預估、評估、因應（例如減輕...）風險，並定期審查。控管者不得透過保險契約來規避風險管理之責任。

1項）。然而，未滿足觸發辦理DPIA義務之事實並不會減少控管者應實施對當事人權利和自由的適當風險管理措施之一般義務。在實務上，此意味著控管者必須不斷評估其運用活動所產生之風險，以確認何種類型之運用「可能對自然人權利和自由造成高風險」。

The following figure illustrates the basic principles related to the DPIA in the GDPR:

下圖說明GDPR中與DPIA相關之基本原則：





A. What does a DPIA address? A single processing operation or a set of similar processing operations.
DPIA著重點為何？單一運用作業或一系列類似運用作業。

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks".* Recital 92 adds that *"there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

DPIA可僅涉及單一資料運用作業。然而，第35條第1項規定「*單一評估可針對一系列類似且呈現相似高風險之運用作業*」。前言第92點補充說明「*在某些情況下，個資保護影響評估之標的不限於單一計畫，是屬較合理且經濟的，例如，當公務機關或機構欲建立共同的應用程式或運用平台，或當數個控管者計畫引進共同的應用程式或跨產業或跨界之運用環境，或為廣泛使用的水平整合活動*」。

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

一份DPIA可用於評估在性質、範圍、背景、目的和風險方面**類似之數個運用作業**。實際上，DPIA旨在系統性的研究對自然人權利和自由可能造成高風險之新情況，因此對已經研究過的案例（例如在特定情況和特定目的下進行之運用作業）即無辦理DPIA之必要性。此種情況可能係使用類似之技術並基於相同之目的蒐集相同種類之資料。例

如，當市政當局的各機關獨自建立類似之CCTV系統時，可辦理一份DPIA，涵蓋不同控管者的運用作業，或是鐵路運營商（單一控管者）可在一份DPIA中涵蓋其所有車站的影音監視。此亦可能適用於由不同資料控管者實施類似運用作業之情形。於此情況下，所提供之DPIA應被共享或可公開取得，於DPIA中所描述之措施必須執行，且須提供僅辦理單一DPIA之正當理由。

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

當運用作業涉及共同控管者時，需精確地定義其各自之義務。DPIA中應指明哪一方負責處理風險及保護當事人權利和自由之各種措施。每個資料控管者皆應於未洩露秘密（例如：保護營業秘密、智慧財產權，商業機密資訊）或揭露弱點之情況下，表達其需求並分享有用資訊。

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

當技術產品（例如硬體或軟體產品）可能由不同的資料控管者進行不同運用作業時，**使用DPIA評估其對資料保護之影響亦有用處**。當然，使用該產品之資料控管者仍有義務關於該特定執行自行辦理DPIA，但可於適當情形下使用由產品供應商準備之DPIA。智能電錶製造商和公用事業公司間之關係可提供示例。每個產品提供者或受託運用者應共享有用資訊，但不至洩露秘密，亦不至因揭露弱點導致安全風險。

B. Which processing operations are subject to a DPIA? Apart from exceptions, where they are "*likely to result in a high risk*".
哪些運用作業須辦理DPIA？除例外情形，當運用「*可能造成高風險*」時。

This section describes when a DPIA is mandatory, and when it is not necessary to carry out a DPIA.
本章節描述何時DPIA為強制性的，以及何時不需辦理DPIA。

Unless the processing operation meets an exception (III.B.a), a DPIA has to be carried out where a processing operation is "*likely to result in a high risk*" (III.B.b).
除非運用作業符合例外情形（III.B.a），否則當運用作業「*可能造成高風險*」時，即必須辦理DPIA（III.B.b）。

a） When is a DPIA mandatory? When processing is "*likely to result in a highrisk*".
何時DPIA為強制性的？當運用「*可能造成高風險*」時。

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[11].
GDPR並未要求每個可能造成自然人權利和自由風險之運用作業皆需辦理DPIA。只有當運用「*可能對自然人權利和自由造成高風險*」之情況下才必須強制辦理DPIA（第35條第1項，第35條第3項加以闡明，並由第35條第4項補充）。此規定在引入新的資料運用技術時尤為重要[11]。

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.
若不確定是否需辦理DPIA，WP29建議仍辦理DPIA，因DPIA係協助控管者遵守資料保護法的有效工具。

Even though a DPIA could be required in other circumstances, Article 35(3) provides some

[11] See recitals 89, 91 and Article 35(1) and (3) for further examples.
有關進一步示例，請參閱前言第89點和第91點以及第35條第1項和第3項。

examples when a processing operation is "*likely to result in high risks*":
儘管在其他情狀下仍可能需要DPIA，第35條第3項提供了當運用作業「*可能造成高風險*」的一些示例：

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the naturalperson*[12]*;*
  (a) 基於自動化運用（包含剖析）對與自然人相關之個人面向進行系統性和廣泛性的評估，且基於該評估所作成之決策將對自然人產生法律效果或類似重大影響[12]*；*
- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10*[13]*;or*
  (b)大規模的運用第9條第1項規定之特種資料，或第10條所規定之與刑事前科及犯罪相關之個人資料[13]*；或*
- *(c) a systematic monitoring of a publicly accessible area on a largescale*".
  (c)於公眾開放區域進行大規模之系統性監控。

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.
如GDPR第35條第3項序文使用「*特別地*」一詞所示，此為例示清單，可能存在未列於清單但具有類似高風險之「高風險」運用作業，這些運用作業亦應受DPIA之約束。基於此原因，下文訂定之標準有時會超出GDPR第35條第3項提供的三個示例的理解範圍。

In order to provide a more concrete set of processing operations that require a DPIA due to

[12]See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".
請參閱前言第71點：「*尤其是分析或預測有關工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、位置或行動等面向，以建立或使用個人剖析*」。
[13] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".
請參閱前言第75點：「*當個人資料運用涉及揭露種族或人種、政治意見、宗教或哲學信仰、工會會員、以及基因資料之運用、有關健康之資料或有關性生活或前科及犯罪或相關安全措施之資料時*」。

their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processing operations[14], the following nine criteria should be considered.

為了提供一套因其固有之高風險而需辦理DPIA之更具體的運用作業，並考量到第35條第1項和第35條第3項第a至c款之特定要件、第35條第4項和前言第71、75和91點應於國家層級制定之清單、以及其他GDPR規範所提及「*可能造成高風險*」之運用作業[14]，應考量以下九項標準。

1. Evaluation or scoring, including profiling and predicting, especially from "*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements*" (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

   評估或評分，包含剖析和預測，尤其是「*關於當事人工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、位置或行動等面向*」（前言第71和91點）。此類情形之示例可包含金融機構依據信用參考資料庫或反洗錢和反恐融資（AML / CTF）或詐欺資料庫篩選其客戶，或是一家直接向消費者提供基因測試的生物科技公司，以評估和預測疾病/健康風險，亦或以網站使用或導覽建立行為或行銷剖析之公司。

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.

   具有法律效果或類似重大影響之自動化決策：當運用目的是為做出有關當事人之決定，且該決定產生「*關於該自然人之法律效果*」或該決定「*類似重大影響*

[14] See e.g. recitals 75, 76, 92, 116.
請參閱如前言第75、76、92、116點。

該自然人」（第35條第3項第a款）。例如，運用可能導致對個人之排除或歧視。若運用對個人影響甚微或沒有影響則與此特定標準不符。與此概念相關之進一步說明將規範於WP29的剖析指引。

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[15]. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

   系統性監控：用於觀察、監測或控制當事人之運用，包括透過網路蒐集之資料或「*於公眾開放區域進行系統性之監控*」（第35條第3項第c款）[15]。此類型之監控會成為一項判斷標準，係因蒐集個人資料時，當事人可能無法得知蒐集者為何人以及其資料將如何被使用。此外，當事人在公開場所（或公眾開放區域）可能無法避免此類運用。

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked

[15]The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):
WP29對「系統性」之解釋，係以下一項或多項情形（請參閱WP29個資保護長指引 16/EN WP 243）：

- occurring according to a system;
  依據一套系統設定而發生；
- pre-arranged, organised or methodical;
  事先安排、有組織性或具一定方法；
- taking place as part of a general plan for data collection;
  為一套整體資料蒐集計畫之一部分；
- carried out as part of a strategy.
  為一項策略執行之一部分。

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.
WP29將「*公眾得接近使用區域*」解釋為對任何大眾開放之任何場所，例如廣場、購物中心、街道、市場、火車站或公共圖書館。

to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

敏感資料或高度私人性質資料：此類資料包括第9條定義之特殊類型個人資料（例如有關個人政治觀點之資訊），及與第10條定義之前科或犯罪相關個人資料。例如綜合醫院保存病人醫療記錄或私人調查員保留違法者之詳細資訊。除GDPR這些規定外，某些類型之資料被視為會對個人權利和自由增加可能的風險。這些個人資料會被認為是敏感的（如同通常對於"敏感"之理解），因其與家庭和私人活動相關聯（如電子通訊秘密應受保護），或因其影響基本權利之行使（如蒐集所在位置之資料會造成自由移動權利之質疑），或因其違反明顯對當事人日常生活造成嚴重影響（如金融資料可能被用於支付詐欺）。在此情況下，資料是否已由當事人或第三方公開是有關聯性的。若預期資料將為某些目的之進一步運用，則可將個人資料已公開之事實視為評估的要素之一。此標準亦可包括諸如個人文件、電子郵件、日記、有筆記記錄功能電子閱讀器中之筆記以及生活日誌應用程式中所包含非常私人之資訊。

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a largescale[16]:

   大規模資料運用：雖然前言第91點提供了一些指導，GDPR並未定義構成大規模之要件。無論如何，WP29建議在決定是否進行大規模運用時，應特別考量以下要素[16]:

   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

[16]See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
請參閱WP29個資保護長指引，16/EN WP 243。

涉及之當事人數，是否達到一定數量或占相關人口之一定比例；

b. the volume of data and/or the range of different data items being processed;
運用之資料量及/或不同資料項目範圍；

c. the duration, or permanence, of the data processing activity;
資料運用作業之期間或持續性；

d. the geographical extent of the processing activity.
運用作業之地理涵蓋範圍。

6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the datasubject[17].
配對或組合資料集：例如源自為不同目的和/或由不同資料控管者實施的兩個或兩個以上的資料運用作業，且其方式將超出當事人之合理期待[17]。

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, *etc.*), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
與弱勢當事人相關之資料（前言第75點）：運用此類型資料之所以成為一項判斷標準，係因其增加當事人和資料控管者間之權力失衡，此意味著當事人可能無法輕易地同意或拒絕其個人資料之運用或行使其權利。弱勢當事人可能包含兒童（兒童可能被認為無法有意識地和深思熟慮地拒絕或同意對其資料之運用）、員工、較弱勢需特殊保護之群體（精神病患者、尋求庇護者或老年人、病患等），以及在任何情況下，會認為當事人與控管者間的關係產生失衡之情事。

8. Innovative use or applying new technological or organisational solutions, like

[17]See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.
請參閱WP29關於目的限制意見中之說明，13/EN WP 203，第24頁。

combining use of finger print and face recognition for improved physical access control, *etc.* The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

創新使用或應用新的技術性或組織性之解決方案，例如結合使用指紋和臉部辨識以改進實體存取控制等。GDPR明確指出（第35條第1項及前言第89點和第91點），使用「*依照現有的技術知識狀態*」（前言第91點）定義下之新技術可觸發辦理DPIA之要求。這是因為使用此類技術會涉及新形式之資料蒐集和使用，並可能對個人之權利和自由產生高風險。實際上，新技術的使用對個人和社會之後果可能是未知的。DPIA將可協助資料控管者理解和處理此類風險。例如，某些「物聯網」(IoT) 應用程式可能會對個人的日常生活和隱私造成重大影響; 因此需要DPIA。

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

   當運用本身「*阻止當事人行使權利或使用服務或契約*」時（第22條和前言第91點）。此情形包括目的在允許、變更或拒絕當事人取得服務或簽訂契約之運用作業。例如銀行依據信用參考資料庫篩選其客戶，以決定是否提供貸款。

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

在多數情況下，當運用符合上述兩項標準時，資料控管者會認為須辦理DPIA。一般而

言，WP29認為當運用符合越多項標準時，越有可能對當事人之權利和自由造成高風險，因此需要DPIA，無論控管者預計採行之措施為何。

However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.
然而，在某些情況下，資料控管者可認為即使運用僅符合其中一項標準亦須辦理DPIA。

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:
以下示例說明如何使用這些標準來評估一個特定的運用作業是否需要DPIA：

Examples of processing **運用之示例**	**Possible Relevant criteria** **可能的相關標準**	**DPIA likely to be required?** **是否可能需要DPIA？**
A hospital processing its patients' genetic and health data (hospital information system). 醫院運用病患之基因和健康資料（醫院資訊系統）。	- Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。 - Data processed on a large-scale. 大規模資料運用。	Yes 是
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates. 使用攝影系統監控高速公路上的駕駛行為。控管者預計使用智能影像分析系統來挑選車輛並自動識別車牌。	- Systematic monitoring. 系統性監控。 - Innovative use or applying technological or organisational solutions. 創新使用或應用技術性或組織性之解決方案	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station,	- Systematic monitoring. 系統性監控。 - Data concerning vulnerable data subjects.	

internet activity, *etc*. 公司系統性地監控員工活動，包括監控員工的個人工作區、網路活動等。	與弱勢當事人相關之資料。	
The gathering of public social media data for generating profiles. 蒐集公眾社交媒體資料以建立剖析檔案。	- Evaluation or scoring. 評估或評分。 - Data processed on a largescale. 大規模資料運用。 - Matching or combining of datasets. 配對或組合資料集。 - Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。	
An institution creating a national level credit rating or fraud database. 建立國家層級的信用等級或詐欺資料庫之機構。	- Evaluation or scoring. 評估或評分。 - Automated decision making with legal or similar significant effect. 具有法律效果或類似重大影響之自動化決策。 - Prevents data subject from exercising a right or using a service or a contract. 阻止當事人行使權利或使用服務或契約。 - Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials 基於歸檔目的，儲存用於研究計畫或臨床試驗之弱勢當事人的假名化個人敏感資料。	- Sensitive data. 敏感資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。 - Prevents data subjects from exercising a right or using a service or a contract. 阻止當事人行使權利或使用服務或契約。	

Examples of processing **運用之示例**	**Possible Relevant criteria** **可能的相關標準**	**DPIA likely to be required?** **是否可能需要DPIA？**
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91). 由「個別醫生、其他健康照護專業人員或律師」運用「病患或客戶之個人資料」（前言第91點）。	- Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質之資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。	No 否
An online magazine using a mailing list to send a generic daily digest to its subscribers. 網路雜誌使用寄件清單向其訂閱戶發送一般每日摘要。	- Data processed on a largescale. 大規模資料運用。	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website. 電子商務網站以在其網站上查看或購買項目的有限剖析，廣告其最佳汽車零件。	- Evaluation or scoring. 評估或評分。	

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

反之，運用作業可能符合上述情況，但控管者仍認為「不太可能造成高風險」。在此情況下，控管者應證明並記錄不辦理DPIA之原因，且應包含/記錄個資保護長之意見。

In addition, as part of the accountability principle, every data controller "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

此外，作為課責原則的一部分，每個資料控管者「*應保有於其職責範圍內運用活動之記錄*」，除其他事項外，包含運用目的、資料類型和資料接收者之描述，以及「*如適用，第32條第1項所述技術性和組織性安全措施之一般說明*」（第30條第1項），並且必須評估是否存在高風險之可能，即使控管者最終決定不辦理DPIA。

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[18]. The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article35(4).

備註：監管機關被要求建立、公開並向EDPB溝通需要DPIA的運用作業清單（第35條第4項）[18]。上述之標準可協助監管機關建立該清單，並在適當時機添加更具體之內容。例如，任何類型的生物特徵資料或兒童資料之運用亦可被視為與依據第35條第4項建立之清單相關聯。

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

   何時不需要DPIA？當運用不太「*可能造成高風險*」或已存在類似之DPIA時，又或該運用是在2018年5月之前獲得授權、或其具有法律依據，或是在不需要DPIA之運用作業清單中。

WP29 considers that a DPIA is not required in the following cases:

[18]In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

在此背景下「*當此類型清單涉及與向當事人提供商品或服務或於數個成員國監控其行為相關之運用活動，或對歐盟境內個人資料的自由流通產生實質性影響時，權責監管機關應適用第63條所述之一致性機制*」（第35條第6項）。

WP29認為在下列情況下不需要DPIA：

- **where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons"** (Article 35(1));
  當運用不太「可能對自然人權利和自由造成高風險」時（第35條第1項）；
- **when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.** In such cases, results of DPIA for similar processing can be used (Article35(1)[19]);
  當運用之性質、範圍、背景和目的與已辦理之DPIA非常相似時。在此情形下，可使用類似運用之DPIA的結果（第35條第1項[19]）；
- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed[20] (see III.C);
  在未改變特定條件下，當監管機關已於2018年5月前檢查過運用作業時[20]（請參閱III.C）；
- **where a processing operation,** pursuant to point (c) or (e) of article 6(1), **has a legal basis** in EU or Member State law, where the law regulates the specific processing operation **and where a DPIA has already been carried out** as part of the establishment of that legal basis (Article 35(10))[21], except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;
  當依據第6條第1項第c款或第e款之**運用作業**在歐盟或成員國法律中**具有法律依據**，該法律規範了具體運用作業**且已辦竣之DPIA已**作為建構該法律依據之一部分時（第35條第10項）[21]，除非成員國已聲明有必要於運用活動前辦理DPIA；
- **where the processing is included on the optional list (established by the**

[19]"*A single assessment may address a set of similar processing operations that present similar high risks.*"
「單一評估得針對一系列呈現相似高風險之類似運用作業」。

[20] "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).
「*執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效*」（前言第171點）。

[21]When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities.
若係為提供運用之法律依據而在立法階段辦理之DPIA，則可能需要在開始作業前再次檢視，因通過之法規可能會與提案不同，而影響到隱私權及資料保護議題。此外，即使有DPIA，在法規通過時也可能無法對實際運用提供足夠之技術細節描述。在此情況下，於執行實際運用作業前可能仍需辦理特定之DPIA。

supervisory authority) of processing operations for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, *etc*. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with all the relevant requirements of the GDPR.

當運用列於無需DPIA的運用作業選擇性清單（由監管機關建立）中（第35條第5項）。此類清單可能包含應符合該機關指定條件之運用活動，特別是透過指引、特定決策或授權、合規性規則等（例如法國制度下的授權、免責、簡化規則、合規性包裹...）。在此情況下，由權責監管機關重新評估，不需要DPIA，但前提為運用需嚴格屬於該清單中提及之相關程序範圍，並持續完全符合所有GDPR相關要求。

C. What about already existing processing operations? DPIAs are required in some circumstances.

對於現行運用作業之要求為何？在某些情況下需要DPIA。

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

當現行的運用作業可能對自然人之權利和自由造成高風險；及將運用之性質、範圍、背景和目的納入考量時，該風險已發生變化，應辦理DPIA。

A DPIA is not needed for processing operations that have been checked by a supervisory authority or the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

監管機關或個資保護長已依據95/46/EC指令第20條檢視之運用作業，且這些運用作業之實施方式自先前檢視後並未改變者，無須辦理DPIA。實際上，「*執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效*」（前言第171點）。

Conversely, this means that any data processing whose conditions of implementation (scope,

purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

相反的，此意味著當任何資料運用之實施條件（範圍、目的、蒐集之個人資料、資料控管者或接收者之身分、資料留存期、技術性和組織性措施等）自監管機關或個資保護長先前檢查以來已發生變化，且可能造成高風險時，則該運用應辦理DPIA。

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations[22], for example because a new technology has come into use or because personal data is being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned.

此外，在運用作業造成之風險有變化後，可能需要DPIA[22]，例如因新技術之使用或因個人資料被用於其他不同目的。資料運用作業可能快速發展，因而可能出現新的弱點。因此，應注意者為，DPIA之修正不僅有助於持續改進，且對於在不斷變化的環境中保持資料保護水準亦至關重要。當運用作業之組織或社會背景改變時，DPIA也可能變得必要，例如，因某些自動決策之影響變得更加重大，或新的當事人類型變得容易受到歧視。上述每一種示例都可能是導致相關運用作業產生風險變化之要素。

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

相反的，某些變化也可能降低風險。例如，運用作業可逐步發展使決策不再自動化或監控活動不再為系統性的。在此情況下，對風險分析之審查可表明不再需要辦理DPIA。

[22]In terms of the context, the data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats, *etc*.), security measures and international transfers.

背景係指蒐集之資料、目的、功能、運用之個人資料、接收者、資料組合、風險（支援資產、風險來源、潛在影響、威脅等）、安全措施和國際傳輸等方面。

As a matter of good practice, **a DPIA should be continuously reviewed and regularly re-assessed.** Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

作為優良實務做法，**應持續審查DPIA並定期對其進行重新評估。**因此，即使在2018年5月25日時不需要DPIA，作為一般性課責義務之一部分，控管者亦必須在適當之時間點辦理DPIA。

D. How to carry out a DPIA?
如何辦理DPIA？

a) At what moment should a DPIA be carried out? Prior to the processing.
應於何時辦理DPIA？在運用資料之前。

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93)[23]. This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

DPIA應在「*運用前*」（第35條第1項和第35條第10項及前言第90點和第93點）[23]辦理。此與資料保護設計（by design）和預設（by default）原則一致（第25條和前言第78點）。應將DPIA視為協助相關運用的決策工具。

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

在運用作業的設計中應儘早啟動DPIA，即使某些運用作業仍屬未知。在整個運用作業期間，定期更新DPIA將確保資料保護和隱私納入考量，並將鼓勵建立促進合規性之解決方案。隨著開發過程之進展，亦可能需要重複評估中的個別步驟，因某些技術性或組織性措施之選擇可能會影響運用所造成風險之嚴重性或可能性。

The fact that the DPIA may need to be updated once the processing has actually started is not

[23] Except when it is an already existing processing that has been prior checked by the Supervisory Authority, in which case the DPIA should be carried out before undergoing significant changes.
除非是監管機關先前已檢查過之現行運用，否則於進行重大變更前，應辦理DPIA。

a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. **Carrying out a DPIA is a continual process, not a one-time exercise**.

一旦運用開始實際實施，可能需要更新DPIA之事實不是延遲或不辦理DPIA的正當理由。DPIA是一種持續進行的程序，尤其是當運用作業是處於動態且不斷變化之情況下。**辦理DPIA是一種持續之程序，而非一次性作為。**

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors.
誰有義務辦理DPIA？控管者，及其DPO和受託運用者。

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.
控管者需負責確保辦理DPIA（第35條第2項）。DPIA可以由組織內部或外部其他人員完成，然對該任務之最終責任仍歸屬於控管者。

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
當依規定指定DPO時（第35條第2項），**控管者亦須尋求個資保護長（DPO）之建議**，DPO之建議以及控管者之決定應記錄於DPIA中。DPO亦應監督DPIA之辦理成效（第39條第1項第c款）。16/EN WP 243，WP29個資保護長指引提供了進一步的指導。

If the processing is wholly or partly performed by a data processor, **the processor should assist the controller in carrying out the DPIA** and provide any necessary information (in line with Article 28(3)(f)).
若運用之全部或一部係由資料受託運用者實施，則**受託運用者應協助控管者辦理DPIA**，並提供任何必要之資訊（符合第28條第3項第f款）。

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:
「*適當時*」，控管者必須「*尋求當事人或其代理人之意見*」（第35條第9項）。WP29認為：

- those views could be sought through a variety of means, depending on the context (e.g.

a generic study related to the purpose and means of the processing operation, a question to the staff representatives, or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;
可透過各種方式尋求該意見，取決於具體情況（例如，與運用作業目的和方式有關之一般性研究、向員工代表提出之問題、或發送通常的意見調查予資料控管者未來客戶）以確保控管者有法律依據運用尋求此類意見所涉及之任何個人資料。然應指出，同意運用顯然不是尋求當事人意見的一種方式；

- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
若資料控管者的最終決定與當事人之意見不同時，應記錄其繼續實施或停止實施之原因；

- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.
若控管者認為不適合尋求當事人意見，亦應紀錄其理由，例如，將損害公司業務計畫之機密性，或是不符合比例性或是不可實行的。

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:
最後，作為一種良好實務做法，應依據內部政策、程序和規則，定義並記錄其他特定角色和職責，例如：

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the DPIA validation process;
當特定業務單位建議辦理DPIA，該單位應就DPIA提供意見，並參與DPIA確認程序；

- where appropriate, it is recommended to seek the advice from independent experts of different professions[24] (lawyers, IT experts, security experts, sociologists, ethics, *etc.*).
在適當情況下，建議諮詢不同專業的獨立專家[24]（律師、IT專家、安全專家、社

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.
對歐盟隱私影響評估架構之建議，Deliverable D3:http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

會學家、倫理學家等）之意見。

- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article28(3)(f));
  受託運用者之角色和職責必須以合約規定；且DPIA必須在受託運用者之協助下辦理，同時考量運用之性質和受託運用者可得之資訊（第28條第3項第f款）；
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
  若有指定首席資訊安全長（CISO），其與DPO可建議控管者對特定之運用作業辦理DPIA，並應協助利害關係人導入方法論、協助鑑定風險評估品質以及剩餘風險之可接受性，並針對資料控管者背景建構相關知識；
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.
  若有指定首席資訊安全長（CISO），其和/或IT部門，應提供控管者協助，並可依據安全或營運需要，建議對特定運用作業辦理DPIA。

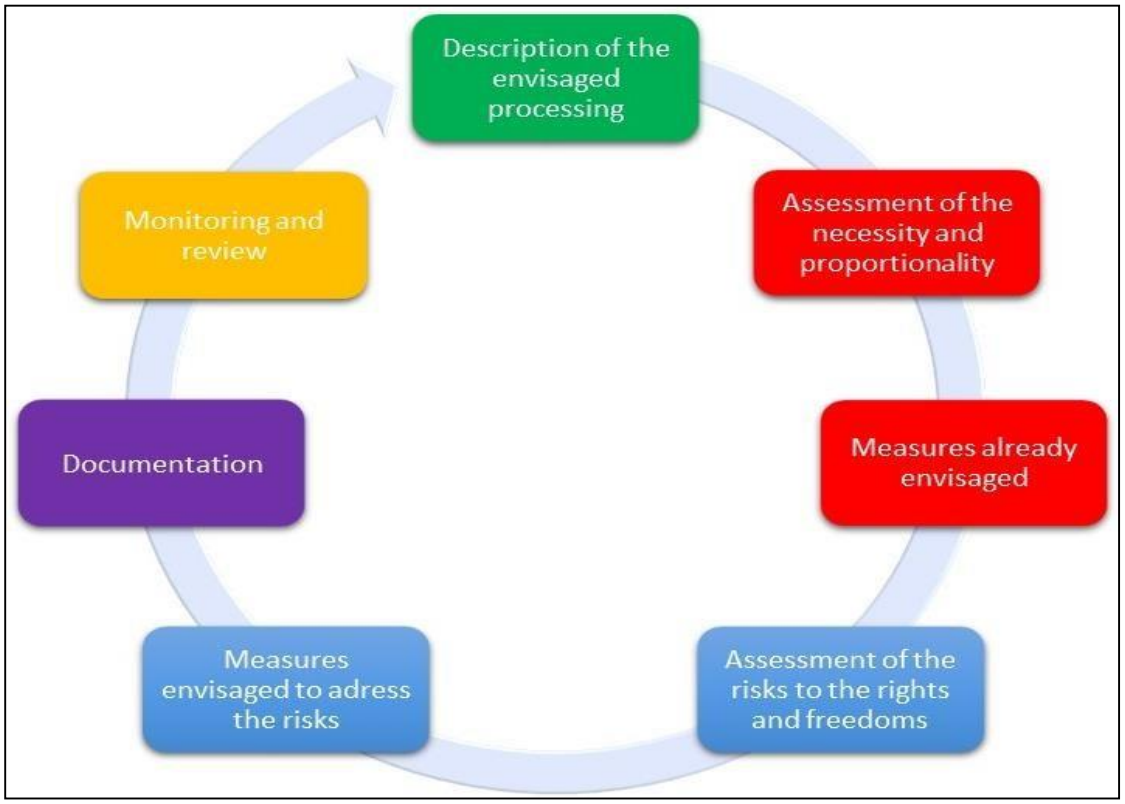
c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.
辦理DPIA之方法論為何？不同之方法論，但共同之標準。

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):
GDPR規定了DPIA至少應包含之要件（第35條第7項，及前言第84點和第90點）：

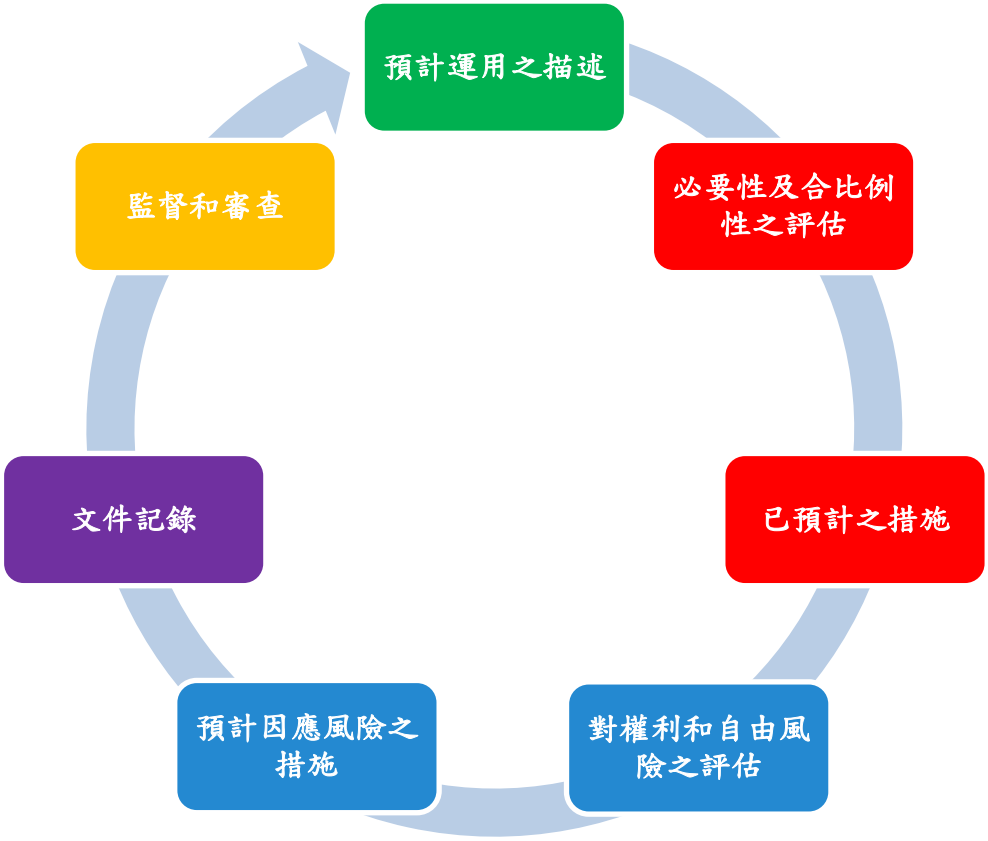
- *"a description of the envisaged processing operations and the purposes of the processing";*
  「預計運用作業和運用目的之描述」；
- *"an assessment of the necessity and proportionality of the processing";*
  「運用之必要性及合比例性之評估」；
- *"an assessment of the risks to the rights and freedoms of data subjects";*
  「對當事人權利和自由風險之評估」；

- *"the measures envisaged to:*
  「預計採取之措施：
  - *"address the risks";*
    「以因應風險」；
  - *"demonstrate compliance with this Regulation".*
    「以證明遵守本規則」

The following figure illustrates the generic iterative process for carrying out a DPIA[25]:
下圖說明辦理DPIA的一般重複循環程序[25]：



[25]It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.
必須強調，此處描述之程序是重複循環性的：實際上，很可能在DPIA完成前需多次重複進行各個階段。



Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.

在評估資料運用作業之影響時，必須考量（第35條第8項）行為守則（第40條）之遵守。若行為守則適用於運用作業，則可用於證明已選擇或實施適當之措施。亦應考量用以證明控管者和受託運用者遵守GDPR運用作業之認證、標章和標誌（第42條），以及具有約束力之企業守則（BCR）。

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. The DPIA implementation is therefore scalable. This means that even a

small data controller can design and implement a DPIA that is suitable for their processing operations.

GDPR中所有相關要求為設計和辦理DPIA提供了廣泛性的通用架構。DPIA的實際辦理將取決於GDPR之要求，並可透過更詳盡的實務指導進行補充。因此，DPIA之辦理是可延展的。此意味著即使是小規模的資料控管者亦可設計和辦理適合其運用作業之DPIA。

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well- defined components of risk management (e.g. ISO 31000[26]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following processes, by:

GDPR前言第90點概述了DPIA所需之各項構成要素，這些構成要素與風險管理（例如ISO 31000[26]）明確定義之構成要素重疊。以風險管理術語來說，DPIA旨在透過以下程序「管理」自然人之權利和自由「風險」：

- establishing the context: "taking into account the nature, scope, context and purposes of the processing and the sources of the risk";
  建立背景：「將運用之性質、範圍、背景和目的以及風險來源納入考量」；
- assessing the risks: "assess the particular likelihood and severity of the high risk";
  評估風險：「評估高風險之特殊可能性和嚴重性」；
- treating the risks: "mitigating that risk" and "ensuring the protection of personal data", and "demonstrating compliance with this Regulation".
  因應風險：「降低風險」和「確保個人資料之保護」，以及「證明遵守本規則」。

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security). Conversely, risk management in other fields (e.g. information security) is focused on the organization.

備註：GDPR下之DPIA是一種管理當事人權利風險之工具，因此如同在某些領域（例如社會安全）之情況，需採取當事人觀點。反之，其他領域之風險管理（例如資訊安全）則著重於組織面。

[26]Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).
風險管理程序：溝通和諮詢、建立背景、風險評估、風險處理、監控和審查（請參閱ISO 31000預先審查中之條款和定義，及目錄）：https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.
GDPR提供資料控管者決定DPIA結構和形式之彈性，以便與現有的工作實務相互配合。歐盟和全世界有許多不同的既定程序，皆考量到前言第90點中所描述之構成要素。然而，無論其形式為何，DPIA必須是對風險的真正評估，允許控管者對該風險採取因應措施。

Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR. In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. **It is up to the data controller to choose a methodology, but this methodology should be compliant with the criteria provided in Annex2**.
可使用不同之方法論（請參閱附錄1資料保護和隱私影響評估方法論示例）來協助執行GDPR中規定之基本要求。為允許這些不同方法存在，同時使控管者得以遵守GDPR之規範，因此列出共同標準（請參閱附錄2）。其釐清本規則之基本要求，但為不同的執行模式提供足夠的空間。這些標準可用於證明特定的DPIA方法論符合GDPR要求之標準。**雖然是由資料控管者選擇方法論，但該方法論應符合附錄2中提供之標準。**

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.
WP29鼓勵發展特定部門(sector-specific)的DPIA架構。因可利用特定之部門知識，使DPIA得因應特定類型運用作業之細節（例如：特定類型之資料、公司資產、潛在影響、威脅、措施）。此意味著DPIA可因應特定經濟部門，或使用特定技術或實施特定類型之運用作業時所出現之問題。

Finally, where necessary, "*the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation*" (Article 35(11)[27]).
最後，在必要時，「*控管者應至少於運用作業所造成之風險發生變化時，審查評估運用之實施是否符合個資保護影響評估*」（第35條第11項[27]）。

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.
是否有義務公布DPIA？沒有，但公布摘要內容可促進信任，且若因事先諮詢或DPA之要求，則必須將完整的DPIA提供予監管機關。

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.
公布DPIA並非GDPR之法律要求，而係控管者之決定。然而，控管者應考量至少公布部分內容，例如DPIA之摘要或結論。

The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.
該程序之目的可能是在協助促進對控管者運用作業之信任，並展現其課責性和透明化。當大眾受到運用作業影響時，公布DPIA是一種非常良好的實務範例。特別是在政府機關辦理DPIA之情況下。

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.
公布之DPIA不需包含整份評估文件，特別是當DPIA可能涉及有關資料控管者安全風險之特定資訊或洩露商業機密或商業敏感資訊時。在此情況下，公布的版本可僅包含DPIA主要評估結果之摘要，或甚至僅為已辦理DPIA之聲明。

Moreover, where a DPIA reveals high residual risks, the data controller will be required to

[27] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.
第35條第10項明確排除第35條第1至7項之適用。

seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice[28], and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents.

此外，當DPIA顯示高剩餘風險時，資料控管者將被要求事先諮詢監管機關對該運用之意見（第36條第1項）。在此情況下，必須完整提供DPIA（第36條第3項第e款）。依據各會員國於公開取得官方文件之原則，監管機關得提供建議[28]，且不會損害商業秘密或揭露安全漏洞。

E. <u>When shall the supervisory authority be consulted? When the residual risks are high.</u>

<u>何時應諮詢監管機關？當有高剩餘風險時。</u>

As explained above:

如上所述：

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;

  當運用作業「*可能對自然人權利和自由造成高風險*」時，需要DPIA（第35條第1項，請參閱III.B.a）。例如，大規模運用健康資料被認為可能造成高風險，並且需要DPIA；

- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[29] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, *etc*.) in addition to existing policies (notice, consent, right of access, right to object, *etc*.).

  因此，資料控管者有責任評估當事人權利和自由之風險，並確認可將此些風險

[28] Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2).
只有當監管機關認為預計之運用不符合第36條第2項規定之規定時，才需向控管者提出書面建議。

降低至可接受程度之預計措施[29]及證明遵守GDPR（第35條第7項，請參閱III.C.c）。例如除現有政策外（通知、同意、近用權、拒絕權等），在筆記型電腦上儲存個人資料時，使用適當的技術性和組織性安全措施（有效全硬碟加密、堅實金鑰管理、適當存取控制、安全備份等）。

In the laptop example above, if the risks have been considered as sufficiently reduced by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) that the data controller must consult the supervisory authority.
在上述筆記型電腦示例中，若資料控管者認為風險已充分降低，並於考量第36條第1項和前言第84點和第94點後，則可在不諮詢監管機關之情況下實施運用。若資料控管者無法充分因應已確認之風險（即剩餘風險仍維持高風險時），資料控管者必須諮詢監管機關。

An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well- known vulnerability is not patched).
無法接受之高剩餘風險的示例包括對當事人可能造成重大甚至無法回復之後果（例如：非法存取資料導致當事人受到生命威脅、裁員、財務危機）和/或當風險似乎明顯會發生時（例如：由於其共享、使用或散布模式以至無法減少造訪資料人數，或尚未修補已知之漏洞）。

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required[30].
若資料控管者找不出足以將風險降低至可接受程度之措施時（即仍維持高剩餘風險時），則需諮詢監管機關[30]。

[29]Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).
包括考量EDPB和監管機關現有之指導，並考量第35條第1項規定的最新技術和實施成本。
[30] Note: "*pseudonymization and encryption of personal data*" (as well as data minimization, oversight mechanisms, *etc*.) are not necessarily appropriate measures. They are only examples. Appropriate measures depend on the context and the risks, specific to the processing operations.
備註：「*個人資料之假名化和加密*」（以及資料最小化、監督機制等）不一定為適當之措施。僅可做為示例。適當措施取決於運用作業之背景和風險。

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).
此外，若成員國法律要求，當控管者實施之運用涉及公共利益時，包括與社會保護和公共衛生相關之運用，控管者必須就該運用諮詢監管機關，和/或得到監管機關事先授權（第36條第5項），則控管者必須諮詢監管機關。

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.
但仍應說明，無論是否需要依據剩餘風險程度諮詢監管機關，保留DPIA記錄並在適當時更新DPIA之義務仍然存在。

IV. Conclusions and recommendations
結論和建議

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.
DPIA是資料控管者實施符合GDPR之資料運用系統的有效方式，且對某些類型之運用作業可能為強制性的。DPIA具有可延展性，可採用不同之形式，但GDPR對有效的DPIA設定了基本要求。資料控管者應將辦理DPIA視為有助於法律遵循的有效且積極之行動。

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".
第24條第1項規定了控管者遵守GDPR之基本責任：「*考量運用之性質、範圍、背景和目的，以及不同可能性與嚴重性對自然人的權利及自由造成之風險，控管者應採取適當的技術性和組織性措施，確保並得以證明依本規則執行運用。必要時應檢視並更新*

這些措施」。

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.
當預計或正在實施高風險資料運用時，DPIA是遵守本規則之關鍵要素。此意味著資料控管者應使用本指引中規定之標準來確認是否須辦理DPIA。資料控管者內部政策可增列GDPR法律要求以外之標準於此清單中。如此可使當事人和其他資料控管者有更充足之信任和信心。

Where a likely high risk processing is planned, the data controller must:
當規劃可能造成高風險之運用時，資料控管者必須：

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:
  選擇符合附錄2標準之DPIA方法論（附錄1中提供之示例），或指定並執行符合以下要件之系統性之DPIA程序：
  - is compliant with the criteria in Annex2;
    符合附錄2中之標準；
  - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
    依據內部程序、環境和文化，整合至現有之設計、開發、變更、風險和營運審核程序中;
  - involves the appropriate interested parties and clearly define their responsibilities (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, *etc*.);
    納入適當利益關係人並明確界定其職責（控管者、DPO、當事人或其代理人、業務、技術服務、受託運用者、資訊安全長等）；
- provide the DPIA report to the competent supervisory authority when required to do so;
  於必要時向權責監管機關提供DPIA報告；
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;

在無法決定足以減輕高風險之措施時，諮詢監管機關；

- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
  定期檢視DPIA及其評估之運用，至少在運用作業所造成之風險發生變化時；
- document the decisions taken.
  記錄所採取之決定。

Annex 1 – Examples of existing EU DPIA frameworks

附錄1 –現行歐盟DPIA架構示例

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

GDPR並未明定必須遵循之DPIA程序，而是允許資料控管者在考量第35條第7項所描述之組成要素下，導入一個可補足其現行作業活動之架構。此架構可以是資料控管者所制定的，或是特定行業之共同架構。由歐盟DPA和歐盟特定部門先前所發展並公布之架構，包括（但不限於）：

Examples of EU generic frameworks:

歐盟通用架構示例：

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  德國：標準資料保護模型，V.1.0 - 試用版本，2016[31]。
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para unaEvaluación de Impactoen la Protección de DatosPersonales (EIPD)*, Agenciaespañola de protección de datos (AGPD), 2014.
  西班牙：*個人個資保護影響評估指南（EIPD）*，西班牙資料保護機關（AGPD），2014。
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  法國：*隱私影響評估（PIA）*，國家資訊及自由委員會（CNIL），2015。
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information

[31] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.
2016年11月9日至10日，聯邦和各州在Kühlungsborn （屈隆斯博恩）的獨立資料保護機關會議，92票一致且無異議通過（巴伐利亞邦棄權）。

Commissioner's Office (ICO),2014.

英國：*執行隱私影響評估實踐準則*，資訊主委辦公室（ICO），2014。

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:

歐盟特定部門架構示例：

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[32].

  RFID應用之隱私和個資保護影響評估架構[32]。

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[33]

  智慧電網和智慧計量系統之個資保護影響評估範本[33]。

  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[34]).

國際標準亦可為辦理DPIA之方法論提供指引（ISO/IEC 29134[34]）。

---

[32]See also :

請另參閱：

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification.
  2009年5月12日執委會關於以無線射頻辨識應用於執行隱私和資料保護原則之建議。
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.
  9/2011意見，關於RFID應用之隱私和個資保護影響評估架構之產業提案修正版。
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33]See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

請另參閱07/2013意見，關於由執委會智慧電網工作特別小組專家第2組編寫關於智慧電網和智慧計量系統之個資保護影響評估範本（「DPIA範本」）。

[34] ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

ISO/IEC 29134（計畫），*資訊科技 - 安全技術 - 隱私影響評估 – 指引*，國際標準化組織（ISO）。

Annex 2 – Criteria for an acceptable DPIA

附錄2 – 可接受之DPIA標準

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

WP29就資料控管者可用以評估所辦理之DPIA，或辦理DPIA之方法論，是否足以全面符合GDPR，提出了以下標準：

- ☐ a systematic description of the processing is provided (Article35(7)(a)):
  提供對運用作業系統性之描述（第35條第7項第a款）：
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
    運用之性質、範圍、背景和目的已納入考量（前言第90點）；
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
    已記錄之個人資料、接收者和個人資料儲存期限；
  - ☐ a functional description of the processing operation is provided;
    已提供運用作業之功能性描述；
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
    已確認個人資料所依賴之資源（硬體、軟體、網路、人員、文件或文件傳輸管道）；
  - ☐ compliance with approved codes of conduct is taken into account (Article35(8));
    已遵循經核准之行為守則（第35條第8項）；
- ☐ necessity and proportionality are assessed (Article35(7)(b)):
  已評估必要性及合比例性（第35條第7項第b款）：
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    確認為遵守本規則而預計採行之措施（第35條第7項第d款和前言第90點），同時考量到：
    - ☐ measures contributing to the proportionality and the necessity of the

processing on the basis of:

如下有助於使運用符合比例性和必要性之措施：

- ☐ specified, explicit and legitimate purpose(s) (Article5(1)(b));
  特定、明確及合法之目的（第5條第1項第b款）；
- ☐ lawfulness of processing (Article6);
  運用之合法性（第6條）；
- ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  適當、相關且限於必要之資料（第5條第1項第c款）；
- ☐ limited storage duration (Article5(1)(e));
  有限之儲存期限（第5條第1項第e款）；

☐ measures contributing to the rights of the data subjects:

有助於當事人權利之措施：

- ☐ information provided to the data subject (Articles 12, 13 and14);
  提供予當事人之資訊（第12、13和14條）；
- ☐ right of access and to data portability (Articles 15 and20);
  近用及資料可攜權（第15條和第20條）；
- ☐ right to rectification and to erasure (Articles 16, 17 and19);
  更正和刪除權（第16、17和19條）；
- ☐ right to object and to restriction of processing (Article 18, 19 and21);
  拒絕和限制運用權（第18、19和21條）；
- ☐ relationships with processors (Article 28);
  與受託運用者之關係（第28條）；
- ☐ safeguards surrounding international transfer(s) (Chapter V);
  國際傳輸之安全維護措施（第五章）；
- ☐ prior consultation (Article36).
  事前諮詢（第36條）。

☐ <u>risks to the rights and freedoms of data subjects are managed</u> (Article35(7)(c)):

已管理當事人權利和自由之風險（第35條第7項第c款）：

- ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  鑑別風險來源、本質、特殊性與嚴重性（請參閱前言第84點），或更具體來說，從當事人之觀點來看待每項風險（非法存取、未預期之修改和資料滅失）：
  - ☐ risks sources are taken into account (recital90);
    已考量風險來源（前言第90點）；
  - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    已確認當發生包含非法存取、未預期之修改和資料滅失等事件時，對當事人權利和自由之潛在影響；
  - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    已確認可能導致非法存取、未預期之修改和資料滅失之威脅；
  - ☐ likelihood and severity are estimated (recital90);
    已評估可能性和嚴重性（前言第90點）；
- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
  已決定預計用以因應這些風險之措施（第35條第7項第d款和前言第90點）；

☐ interested parties are involved:
利益關係人已參與：

- ☐ the advice of the DPO is sought (Article35(2));
  已尋求DPO之建議（第35條第2項）；
- ☐ the views of data subjects or their representatives are sought, where appropriate (Article35(9)).
  已酌情徵詢當事人或其代理人之意見（第35條第9項）。

ARTICLE 29 DATA PROTECTION WORKING PARTY
第29條個資保護工作小組

17/EN
WP251rev.01

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679
關於第 2016/679 號規則(GDPR)中的自動化個人決策和剖析之指引

Adopted on 3 October 2017

2017 年 10 月 3 日通過

As last Revised and Adopted on 6 February 2018

2018 年 2 月 6 日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm
網址：http://ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

依歐洲議會與歐盟理事會 1995 年 10 月 24 日通過之 95/46/EC 指令而設立，

having regard to Articles 29 and 30 thereof,

基於該指令第29條及第30條，

having regard to its Rules of Procedure,

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

TABLE OF CONTENTS 目錄

I. Introduction
導言

The General Data Protection Regulation (the GDPR), specifically addresses profiling and automated individual decision-making, including profiling.[1]

一般資料保護規則（GDPR）特別規範剖析和自動化個人決策（包含剖析）。[1]

Profiling and automated decision-making are used in an increasing number of sectors, both private and public. Banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making.

使用剖析和自動化決策之產業逐漸增加，包含私人或公共部門。銀行和金融、醫療保健、稅務、保險、行銷和廣告僅是幾個經常使用剖析協助決策之行業示例。

Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms.

技術的進步以及大數據分析、人工智慧和機器學習的能力使得剖析建檔和做出自動化決策變得更加容易，且有對於個人的權利和自由產生重大影響之可能。

The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, an d repealing Directive 95/46/EC. Profiling and automated individual decision-making are also covered by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. While these guidelines focus on profiling and automated individual decision-making under the GDPR, the guidance is also relevant regarding the two topics under Directive 2016/680, with respect to their similar provisions. The analysis of specific features of profiling and automated individual decision-making under Directive 2016/680 is not included in these guidelines, since guidance in this respect is provided by the Opinion WP258 "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", adopted by WP29 on 29 November 2017 This Opinion covers automated individual decision - making and profiling in the context of law enforcement data processing at pages 11-14 and is available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178
2016年4月27日歐洲議會和歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，制定第2016/679號規則(EU)，並廢除第95/46 / EC號指令。2016年4月27日歐洲議會和理事會第2016/680號指令(EU)亦涵蓋了剖析和自動化個人決策，關於權責機關為預防、調查、偵查或起訴刑事犯罪或執行刑事處罰而運用個人資料時，對自然人之保護與確保該資料之自由流通。雖然本指引著重於GDPR下之剖析和自動化個人決策，但本指導與第2016/680號指令中就此兩項主題之類似規定亦為相關。第2016/680號指令中之剖析和自動化個人決策的具體特徵分析並未涵蓋於本指引中，因WP258意見「關於執法指令之關鍵議題意見」(EU 2016/680)提供了此方面之指導，WP29於2017年11月29日通過。此意見第11-14頁涵蓋了執法資料運用背景下之自動化個人決策和剖析，請參閱：
http：//ec.europa.eu/newsroom/article29/item-detail.cfm？ITEM_ID=610178

personality or behaviour, interests and habits to be determined, analysed and predicted.
網路和物聯網（IoT）設備上個人資料之廣泛可得性以及發現關聯性和建立連結之能力，使得當事人之個性或行為、興趣和習慣等各個面向皆可被確認、分析和預測。

Profiling and automated decision-making can be useful for individuals and organisations, delivering benefits such as:
剖析和自動化決策對個人及組織是有幫助的，其可帶來之益處如：

- increased efficiencies; and
  提高效率；及
- resource savings.
  節省資源。

They have many commercial applications, for example, they can be used to better segment markets and tailor services and products to align with individual needs. Medicine, education, healthcare and transportation can also all benefit from these processes.
剖析和自動化決策具有許多商業應用，例如，可用以妥善劃分市場、訂製服務及符合個人化需求之產品。醫學、教育、醫療保健和交通運輸亦受益於這些運用。

However, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards.
然而，剖析和自動化決策可能會對需要適當安全維護措施之個人權利和自由造成重大風險。

These processes can be opaque. Individuals might not know that they are being profiled or understand what is involved.
這些運用可能是不透明的。個人可能無法得知正在被剖析或理解其所涉及之內容。

Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination.
剖析可能將現有的刻板印象和社會隔離永久化。剖析亦可能將某個人鎖定於特定類型，並將其限於被建議之偏好。此亦會損害其選擇某些產品或服務（如書籍、音樂或新聞來源）之自由。在某些情況下，剖析可能會造成預測之不準確。而於其他情況中，剖析可能造成拒絕提供服務和產品以及不合理歧視。

The GDPR introduces new provisions to address the risks arising from profiling and automated

decision-making, notably, but not limited to, privacy. The purpose of these guidelines is to clarify those provisions.
GDPR引進了新的規定以因應剖析和自動化決策所帶來之風險，尤其是隱私權(但不以此為限)。本指引之目的即是在闡明這些規定。

This document covers:
本文件涵蓋：

- Definitions of profiling and automated decision-making and the GDPR approach to these in general – Chapter II
  剖析和自動化決策之定義以及GDPR對此之總體態度 - 第二章
- General provisions on profiling and automated decision-making – Chapter III
  剖析和自動化決策之一般規定 - 第三章
- Specific provisions on solely automated decision-making defined in Article 22 - Chapter IV
  第22條定義之純自動化決策具體規定- 第四章
- Children and profiling – Chapter V
  兒童和剖析 - 第五章
- Data protection impact assessments and data protection officers– Chapter VI
  個資保護影響評估和個資保護長 - 第六章

The Annexes provide best practice recommendations, building on the experience gained in EU Member States.
附錄依據歐盟成員國之經驗提供最佳實務作法建議。

The Article 29 Data Protection Working Party (WP29) will monitor the implementation of these guidelines and may complement them with further details as appropriate.
第29條個資保護工作小組（WP29）將監督本指引之執行情況，並可酌情補充進一步細節。

II. Definitions
定義

The GDPR introduces provisions to ensure that profiling and automated individual decision-making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' rights; for example:
GDPR引進了某些規定以確保剖析和自動化個人決策（無論是否包含剖析）之使用方式不

會對個人權利產生不合理之影響; 例如：

- specific transparency and fairness requirements;
  具體透明和公正性之要求；
- greater accountability obligations;
  更高之課責義務；
- specified legal bases for the processing;
  運用之具體法律基礎；
- rights for individuals to oppose profiling and specifically profiling for marketing; and
  當事人拒絕剖析和專為行銷目的之剖析的權利；及
- if certain conditions are met, the need to carry out a data protection impact assessment.
  若滿足某些要件，則需辦理個資保護影響評估。

The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals.
GDPR並非只著重自動運用或剖析結果所為之決策。GDPR適用於為建立剖析檔案而蒐集之資料，以及這些剖析對當事人之應用。

A. Profiling
剖析

The GDPR defines profiling in Article 4(4) as:
GDPR於第4條第4款將剖析定義為：

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
> 任何形式之個人資料自動化運用，包含使用個人資料評估與自然人相關之某些個人面向，尤其是分析或預測有關該自然人在工作上之表現、經濟狀況、健康、個人偏好、興趣 、可信度、行為、所在位置或移動；

Profiling is composed of three elements:

剖析由三項要件組成：

- it has to be an *automated* form of processing;
  剖析必須是一種*自動化*的運用形式；
- it has to be carried out *on personal data*; and
  剖析必須是*針對個人資料*之執行；及
- the objective of the profiling must be *to evaluate personal aspects* about a natural person.
  剖析之目的必須是*評估*關於自然人之*個人面向*。

Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.
第4條第4款指的是「任何形式之自動化運用」而非「純」自動化之運用（請參閱第22條）。剖析必須涉及某種形式之自動化運用 – 即使人為參與並不一定會將活動排除於此定義之外。

Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.
剖析係一種可能涉及一系列統計衍繹之程序。剖析通常用於對人的預測，基於統計上相似之他人特質，使用各種來源之資料以推論個人。

The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse *or* make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.
GDPR表示，剖析係為評價個人面向而自動化運用個人資料，尤其是分析或預測個人。使用「評價」一詞表示剖析涉及對某人進行某種形式之評估或判斷。

A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.
基於已知特徵（例如年齡、性別和身高）而對當事人進行簡單分類並不一定會導向剖析。

此應取決於分類之目的。例如，企業可能希望依據年齡或性別對其客戶進行分類以用於統計目的，並獲得對客戶的整體概觀，而無需做出任何預測或得出與個人相關之任何結論。在此情況下，其目的並非評估當事人特徵，因此不屬於剖析。

The GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec (2010)13[2] (the Recommendation), as the Recommendation *excludes* processing that does not include inference. Nevertheless the Recommendation usefully explains that profiling may involve three distinct stages:
GDPR雖受歐盟理事會第CM / Rec（2010）13號建議書[2]（下稱建議書）啟發，但因建議書排除不涉推論之運用，因此二者對剖析的定義有所不同。然而，該建議書有效地解釋了剖析可能涉及之三種不同階段：

- data collection;
  資料蒐集；
- automated analysis to identify correlations;
  自動化分析以識別關聯性；
- applying the correlation to an individual to identify characteristics of present or future behaviour.
  將關聯性應用於個人以識別目前或未來行為之特徵。

Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.
控管者在執行剖析時將需確保符合GDPR對上述所有階段規定之要求。

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:
從廣義上來說，剖析意味著蒐集有關個人（或一群個人）之資訊並評價其特徵或行為模式，以便將其歸納入某個類型或群體，尤其是分析和/或預測，例如，他們的：

- ability to perform a task;

[2] Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe 23 November 2010. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf . Accessed 24 April 2017
歐盟理事會。保護個人在剖析之背景下自動化運用個人資料。第 CM / Rec（2010）13 號建議和解釋備忘錄。歐盟理事會 2010 年 11 月 23 日。https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf . 瀏覽日期：2017年4月24日。

執行任務之能力；

- interests; or
  興趣；或
- likely behaviour.
  可能之行為。

Example
示例

A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests.
資料仲介代表其客戶或基於自身目的，從不同的公共和私人來源蒐集資料。資料仲介編輯資料以建立個人剖析檔案，並將其分類。仲介出售此資訊予希望改進其產品和服務之定位的公司。資料仲介透過依個人興趣分類之方式進行剖析。

Whether or not there is automated decision-making as defined in Article 22(1) will depend upon the circumstances.
是否存在第22條第1項所定義之自動化決策將取決於具體情況。

B. Automated decision-making
自動化決策

Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example:
自動化決策具有不同之範圍，且可能與剖析部分重疊或因剖析而產生。純自動化決策係指在沒有人為參與之情況下，透過技術性方式做出決策之能力。自動化決策可以任何類型之資料為基礎而產生，例如：

- data provided directly by the individuals concerned (such as responses to a

questionnaire);
直接由相關個人提供之資料（如對調查問卷之回覆）；

- data observed about the individuals (such as location data collected via an application);
  觀察個人所得之資料（例如透過應用程式蒐集之位置資料）；
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).
  衍生或推論之資料，例如由已建立之個人剖析檔案（例如，信用評分）。

Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.
不論有無剖析皆可做出自動化決策；而在無自動化決策之情況下亦可執行剖析。然而，剖析和自動化決策不一定是分開的活動。某一個在剛開始時只是簡單的自動化決策程序，視其資料之使用方式，可能成為基於剖析而為之決策。

Example
示例

Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision- making process that does not necessarily involve profiling.
僅依高速攝影機取得之證據而裁處之超速罰款，是一種不一定涉及剖析之自動化決策程序。

It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.
然而，若長時間監控個人之駕駛習慣，則可能成為依據剖析之決策，例如，若罰鍰裁處額度涉及其他因素評估之結果，如超速是否為重複犯行或駕駛人最近是否有其他的交通違規行為。

Decisions that are not solely automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful

intervention carried out by humans before any decision is applied to an individual.
非純自動化決策亦可能包含剖析。例如，在給予抵押貸款前，銀行可能會考量借款人之信用評分，而在對個人作出任何決定前，進行其他有意義之人為參與。

C. How the GDPR addresses the concepts
GDPR如何處理這些概念

There are potentially three ways in which profiling may be used:
可能有三種使用剖析之方式：

(i) general profiling;
一般剖析；

(ii) decision-making based on profiling; and
基於剖析所為之決策； 及

(iii) *solely* automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject (Article 22[1]).
對當事人產生法律效果或類似重大影響之包含剖析的*純*自動化決策（第22條第1項）。

The difference between (ii) and (iii) is best demonstrated by the following two examples where an individual applies for a loan online:
（ii）和（iii）之間的差異可以個人申請線上貸款的兩個示例做最好的說明：

- a human decides whether to agree the loan based on a profile produced by purely automated means(ii);
依據純自動化方式之剖析，由人為決定是否同意貸款（ii）；
- an algorithm decides whether the loan is agreed and the decision is automatically delivered to the individual, without any prior and meaningful assessment by a human (iii).
以演算法決定是否同意貸款，且自動傳遞該決定予該個人，而無需任何事前且有意義的人為評估（iii）。

Controllers can carry out profiling and automated decision-making as long as they can meet all the principles and have a lawful basis for the processing. Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling, defined in Article 22(1).
控管者只要能符合所有原則並具有運用之合法基礎，即可進行剖析和自動化決策。在第22

條第1項定義之純自動化決策(包含剖析)情況下，需適用額外之安全維護措施和限制。

Chapter III of these guidelines explains the GDPR provisions for *all* profiling and automated individual decision-making. This includes decision-making processes that are *not* solely automated.
本指引第三章說明GDPR對*所有*剖析和自動化個人決策之規定。此包含*非單*純自動化決策程序。

Chapter IV of these guidelines explains the specific provisions that *only* apply to solely automated individual decision-making, including profiling.[3] A general prohibition on this type of processing exists to reflect the potential risks to individuals' rights and freedoms.
本指引第四章針對*僅*適用於純自動化個人決策(包含剖析)之具體規定進行說明。[3]為反映個人權利和自由之潛在風險，一般禁止此類運用。

III. General provisions on profiling and automated decision-making
關於剖析和自動化決策之一般規定

This overview of the provisions applies to all profiling and automated decision-making. Additional specific provisions set out in Chapter IV apply if the processing meets the definition in Article 22(1).
此規定之概述適用於所有剖析和自動化決策。若運用符合第22條第1項之定義，則適用第IV章中之額外具體規定。

A. Data protection principles
資料保護原則

The principles are relevant for all profiling and automated decision-making involving personal data.[4] To aid compliance, controllers should consider the following key areas:
這些原則與涉及個人資料之所有剖析和自動化決策相關。[4]為協助其合規，控管者應考量以下關鍵面向：

1. Article 5(1) (a) - Lawful, fair and transparent

[3] As defined in Article 22(1) of the GDPR.
如GDPR第22條第1項所定義。

[4] GDPR – Recital 72 "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles."
GDPR－ 前言第 72點「剖析需符合本規則有關個人資料運用之規定，例如運用之法律依據或資料保護原則。」

第 5 條第 1 項第 a 款 - 合法、公正和透明化

Transparency of processing[5] is a fundamental requirement of the GDPR.
運用之透明度[5]為GDPR之基本要求。

The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.
當事人通常無法察覺剖析之程序。其藉由建立有關個人之衍生或推論資料運作 － 此一「新的」個人資料並非由當事人本身直接提供。個人具有不同程度之理解能力，且可能發現要理解剖析和自動化決策程序中所涉及之複雜技術是具有挑戰性的。

Under Article 12.1 the controller must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data.[6]
依據第12條第1項，控管者必須提供當事人有關其個人資料運用之簡潔、透明、易懂且便於取得之資訊[6]。

For data collected directly from the data subject this should be provided at the time of collection (Article 13); for indirectly obtained data the information should be provided within the timescales set out in Article 14(3).
對於直接從當事人蒐集之資料，該資訊應在蒐集時提供（第13條）；對於間接取得之資料，應在第14條第3項規定之時間範圍內提供資訊。

---

[5] The WP29 Guidelines on transparency cover transparency generally in more detail Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679 WP260, 28 November 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accessed 18 December 2017.
WP29關於透明化之指引更廣泛地涵蓋透明化之更多細節，第29條個資保護工作小組。關於第2016/679號規則中的透明化之指引（WP260），2017年11月28日。http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850，瀏覽日期：2017年12月18日。

[6] Office of the Australian Information Commissioner. Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 says: "Privacy notices have to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. *The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi - layered and user centric privacy notices."* https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles . Accessed 24 April 2017
澳洲資訊委員辦公室。諮詢草案：大數據指南和澳洲隱私原則，第05/2016號指出：「隱私聲明必須清楚、簡單地傳達處理資訊之實際情形，資訊亦須具全面性及足夠之特定性，而使其有意義。正是該項*可更廣泛蒐集個人資訊之技術，亦顯示有機會可提供更加動態、多層次和以用戶為中心之隱私聲明。*」https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy- principles，造訪於2017年4月24日。

Example

示例

Some insurers offer insurance rates and services based on an individual's driving behaviour. Elements taken into account in these cases could include the distance travelled, the time spent driving and the journey undertaken as well as predictions based on other data collected by the sensors in a (smart) car. The data collected is used for profiling to identify bad driving behaviour (such as fast acceleration, sudden braking, and speeding). This information can be cross-referenced with other sources (for example the weather, traffic, type of road) to better understand the driver's behaviour.

某些保險公司依據當事人之駕駛行為提供保險費率和服務。於這些情況下考量之因素可能包含行駛距離、駕駛時間和行程、以及以（智慧）汽車中感應器蒐集之其他資料所為之預測。蒐集之資料用於剖析以識別不良駕駛行為（例如快速加速、緊急煞車和超速）。該資訊可與其他來源（例如天氣、交通、道路類型）做交叉比對，以更加了解駕駛之行為。

The controller must ensure that they have a lawful basis for this type of processing. The controller must also provide the data subject with information about the collected data, and, if appropriate, the existence of automated decision-making referred to in Article 22(1) and (4), the logic involved, and the significance and envisaged consequences of such processing.

控管者必須確保其具有此類運用之合法基礎。控管者亦須提供當事人關於所蒐集資料之資訊，並在適當情況下，提供第22條第1項和第4項所述之自動化決策、所涉邏輯以及該運用之重要性及預見之後果。

The specific requirements surrounding information and access to personal data are discussed in Chapters III (section D) and IV (section E).

有關資訊和近用個人資料之具體要求將在第III章（第D節）和第IV章（第E節）中討論。

Processing also has to be fair, as well as transparent.

運用亦須公正且透明。

Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products. The following example, which would not meet the requirements of Article 5(1)(a), illustrates how unfair profiling can lead to some consumers being offered less attractive

deals than others.

剖析可能係不公正的，並造成歧視，例如，拒絕人們獲得就業機會、信貸或保險，或將其作為過度風險或昂貴之金融產品的目標。以下之示例在不符合第5條第1項第a款要求之情況下，說明了不公正之剖析如何導致某些消費者被給予較不具吸引力之交易條件。

Example

示例

A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products).[7]

資料仲介在未經消費者許可或消費者對相關資料不知情之情況下，將消費者檔案出售予金融公司。這些檔案依消費者之財務脆弱性，將其劃分為不同之類型（名稱包含例如「鄉村和生活貧困者」、「少數民族二線城市掙扎者」、「艱難的開始：年輕單身父母」）或將其「評分」。金融公司為這些消費者提供發薪日貸款和其他「非傳統性」金融服務（高成本貸款和其他有金融風險之產品）。[7]

2. Article 5(1) (b) Further processing and purpose limitation

第 5 條第 1 項第 b 款進一步運用和目的限制

Profiling can involve the use of personal data that was originally collected for something else.

剖析可能涉及使用最初為其他目的蒐集之個人資料。

[7] This example is taken from: United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf . See page ii of the Executive Summary and 12 of the main body of the document in particular. Accessed 21 July 2017

此示例來源：美國參議院，商業、科學和運輸委員會。資料中介產業評論：因行銷目的蒐集、使用和銷售消費者資料，洛克菲勒主席之評核報告，2013 年 12 月 18 日。ttps://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577 / AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry. pdf。 請參閱摘要第 ii 頁，特別是文件本文第 12 頁，瀏覽日期：2017 年 7 月 21 日。

Example

示例

Some mobile applications provide location services allowing the user to find nearby restaurants offering discounts. However, the data collected is also used to build a profile on the data subject for marketing purposes - to identify their food preferences, or lifestyle in general. The data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late. This further use of the location data may not be compatible with the purposes for which it was collected in the first place, and may thus require the consent of the individual concerned.[8]

某些行動電話應用程式提供定位服務，允許用戶可搜尋附近提供折扣的餐廳。然而，為行銷目的，所蒐集之資料亦用於建立當事人剖析檔案 - 以識別其食物偏好或一般的生活方式。當事人預期到其資料將被用於查找餐廳，但未預期到該應用程式僅因識別其回家時間較晚，就接收到外送披薩的廣告。此種定位資料之進一步使用可能與最初蒐集該資料之目的不相容，因而需要該個人之同意。[8]

Whether this additional processing is compatible with the original purposes for which the data were collected will depend upon a range of factors[9], including what information the controller initially provided to the data subject. These factors are reflected in the GDPR[10]and summarised below:

此額外運用是否與蒐集資料之原始目的相容將取決於一系列因素[9]，包含控管者最初提供予當事人之資訊。這些因素反映於GDPR中[10]，並總結如下：

- the relationship between the purposes for which the data have been collected and the purposes of further processing;

  蒐集資料之目的與進一步運用目的間之關係；

- the context in which the data were collected and the reasonable expectations of the data subjects as to their further use;

---

[8] Note that the provisions of the future ePrivacy Regulation may also apply.
應注意未來電子隱私規則之規定亦可能適用。

[9] Highlighted in the Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation,2 April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Accessed 24 April 2017
第 29 條個資保護工作小組第 03/2013 號關於目的限制之意見強調，2013 年 4 月 2 日.http：//ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommended / files / 2013 / wp203_en.pdf，瀏覽日期： 2017 年 4 月 24 日。

[10] GDPR Article 6(4).
GDPR第6條第4款。

蒐集資料之背景以及當事人對該資料進一步使用之合理期待；

- the nature of the data;
  資料之性質；
- the impact of the further processing on the data subjects; and
  進一步運用對當事人之影響；及
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.
  控管者實施之安全維護措施，以確保公正運用並防止對當事人產生任何不當之影響。

3. Article 5(1) (c) Data minimisation

第 5 條第 1 項第 c 款資料最小化

The business opportunities created by profiling, cheaper storage costs and the ability to process large amounts of information can encourage organisations to collect more personal data than they actually need, in case it proves useful in the future. Controllers must make sure they are complying with the data minimisation principle, as well as the requirements of the purpose limitation and storage limitation principles.

剖析所帶來的商機、更低廉的儲存成本和運用大量資訊之能力皆鼓勵組織蒐集比實際所需更多之個人資料，以為將來可能之使用。控管者必須確保其符合資料最小化原則，以及目的限制和儲存限制原則之要求。

Controllers should be able to clearly explain and justify the need to collect and hold personal data, or consider using aggregated, anonymised or (when this provides sufficient protection) pseudonymised data for profiling.

控管者必須能夠清楚地說明和證明蒐集及持有個人資料之必要性，或考量使用聚集的、匿名化、或（當提供足夠保護時）假名化資料進行剖析。

4. Article 5(1) (d) Accuracy

第 5 條第 1 項第 d 款正確性

Controllers should consider accuracy at all stages of the profiling process, specifically when:

控管者應在剖析程序的所有階段考量正確性，尤其是在：

- collecting data;
  蒐集資料；
- analysing data;

分析資料；

- building a profile for an individual; or
  建立個人剖析檔案；或
- applying a profile to make a decision affecting the individual.
  使用剖析檔案做出影響個人之決策。

If the data used in an automated decision-making or profiling process is inaccurate, any resultant decision or profile will be flawed. Decisions may be made on the basis of outdated data or the incorrect interpretation of external data. Inaccuracies may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk.
若自動化決策或剖析程序中使用之資料不正確，任何由此產生之決策或剖析檔案都將存在缺陷。決策可能依據過時之資料或對外部資料之錯誤解釋而產生。不正確性可能導致例如對某人健康、信用或保險風險之不當預測或陳述。

Even if raw data is recorded accurately, the dataset may not be fully representative or the analytics may contain hidden bias.
即使原始資料正確紀錄，其資料集可能不具備完全之代表性，或其分析可能包含隱藏性之偏見。

Controllers need to introduce robust measures to verify and ensure on an ongoing basis that data re- used or obtained indirectly is accurate and up to date. This reinforces the importance of providing clear information about the personal data being processed, so that the data subject can correct any inaccuracies and improve the quality of the data.

控管者需採行強力之措施持續驗證並確保再使用或間接取得之資料係正確和最新的。此加強了提供所運用個人資料的清楚資訊之重要性，如此可使當事人更正任何不正確資料並提高資料品質。

5. Article 5(1) (e) Storage limitation
第 5 條第 1 項第 e 款儲存限制

Machine-learning algorithms are designed to process large volumes of information and build correlations that allow organisations to build up very comprehensive, intimate profiles of individuals. Whilst there can be advantages to retaining data in the case of profiling, since there will be more data for the algorithm to learn from, controllers must comply with the data minimisation principle when they collect personal data and ensure that they retain those personal data for no longer than is necessary for and proportionate to the purposes for which the personal data are processed.
機器學習演算法之設計係在運用大量資訊並建立關聯性，使組織建立非常全面性、私密性

之個人剖析檔案。雖然在剖析時保留資料可能會有好處，因會有更多之資料供演算法學習，然而控管者在蒐集個人資料時必須遵守資料最小化原則，並確保其保留這些個人資料不超過個人資料運用目的所必須，且符合比例性。

The controller's retention policy should take into account the individuals' rights and freedoms in line with the requirements of Article 5(1)(e).
控管者之資料保留政策應依據第5條第1項第e款之要求考量個人之權利和自由。

The controller should also make sure that the data remains updated throughout the retention period to reduce the risk of inaccuracies.[11]
控管者亦應確保資料在保留期限內維持更新，以降低不正確之風險。[11]

B. Lawful bases for processing
運用之合法依據

Automated decision-making defined in Article 22(1) is only permitted if one of the exceptions described in Chapter IV (sections C and D) applies. The following lawful bases for processing are relevant for all other automated individual decision-making and profiling.
只有在適用第IV章（第C和D節）所描述之例外情形下，始允許執行第22條第1項規定之自動化決策。以下運用之法律依據與所有其他自動化個人決策及剖析相關。

1. Article 6(1) (a) consent
第 6 條第 1 項第 a 款同意

Consent as a basis for processing generally is addressed in the WP29 Guidelines on consent.[12] Explicit consent is one of the exceptions from the prohibition on automated decision-making and profiling defined in Article 22(1).
以同意作為運用之法律基礎一般已列入WP29關於同意之指引。[12]明確同意為第22條第1項

[11] Norwegian Data Protection Authority. The Great Data Race – How commercial utilisation of personal data challenges privacy, Report, November 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The- Great-Data-Race/ Accessed 24 April 2017[12] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259, 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
挪威資料保護機關。大數據競賽 - 個人資料商業利用對隱私權之挑戰，報告，2015 年 11 月。Datatilsynet https://www.datatilsynet.no/English/Publications/The- Great-Data-Race / 瀏覽日期：2017 年 4 月 24 日。第 29 條個資保護工作小組，關於第 2016/179 號規則中的同意之指引（WP259），2017 年 11 月 28 日，http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849。 造訪於 2017 年 12 月 18 日。

[12] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259, 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
第29條個資保護工作小組。第2016/679號規則關於同意之指引，WP259，2017年11月28日，http：

禁止自動化決策和剖析的例外情況之一。

Profiling can be opaque. Often it relies upon data that is derived or inferred from other data, rather than data directly provided by the data subject.
剖析可能是不透明的。剖析經常依賴從其他資料衍伸或推論而來之資料，而非由當事人直接提供之資料。

Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for the processing.[13] In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice.
控管者若尋求以同意作為剖析依據，需證明當事人完全理解其同意之內容，且切記同意非必為運用之適當依據。[13]在所有情況下，當事人就預期使用及運用的結果應有足夠之相關資訊，以確保其提供之任何同意係屬告知後的選擇。

2. Article 6(1) (b) – necessary for the performance of a contract
第 6 條第 1 項第 b 款 – 為履行契約所必須

Controllers may wish to use profiling and automated decision-making processes because they:
控管者可能希望使用剖析和自動化決策程序，因其：

- potentially allow for greater consistency or fairness in the decision making process (e.g. by reducing the potential for human error, discrimination and abuse of power);
  可能使決策程序更具一致性或公正性（例如，透過減少潛在之人為錯誤、歧視和濫用權力）；
- reduce the risk of customers failing to meet payments for goods or services (for example by using credit referencing); or
  降低客戶未能支付商品或服務之風險（例如透過信用參考）；或
- enable them to deliver decisions within a shorter time frame and improve efficiency.
  使控管者能在更短的時間內做出決策並提高效率。

Regardless of the above, these considerations alone are not sufficient to show that this type of processing is *necessary* under Article 6(1)(b) for the performance of a contract. As described in the WP29 Opinion on legitimate interest[14], necessity should be interpreted narrowly.

//ec.europa.eu/newsroom/just/document.cfm？doc_id = 48499，瀏覽日期：2017年12月18日。
[13] Ibid.
同上。

無論如何，單單這些考量並不足以證明此種運用係為履行依據第6條第1項第b款之契約*所必須*。正如WP29關於正當利益之意見所述[14]，必要性必須被限縮解釋。

The following is an example of profiling that would *not* meet the Article 6(1)(b) basis for processing.

*以下為未*符合第6條第1項第b款運用依據規定剖析之示例。

Example

示例

A user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website. Even if profiling is specifically mentioned in the small print of the contract, this fact alone does not make it 'necessary' for the performance of the contract.

用户從網路零售商購買某些商品。為了履行契約，零售商必須運用用户之信用卡資訊支付和用户地址以交付貨物。契約之完成並不仰賴依據用户造訪網站之行為而建立用户喜好和生活方式選擇之剖析檔案。即使在契約中以小字體特別提及剖析，僅此一事實並會使剖析成為履行契約所「必須」。

3. Article 6(1) (c) – necessary for compliance with a legal obligation

第 6 條第 1 項第 c 款 – 為履行法律義務所必須

There may be instances where there will be a legal obligation[15] to carry out profiling – for example in connection with fraud prevention or money laundering. The WP29 Opinion on legitimate interests[16] provides useful information about this basis for processing, including the safeguards to be applied.

在某些情況下，可能會依法律義務[15]而執行剖析 - 例如與預防詐欺或洗錢相關聯時。WP29關於正當利益[16]之意見提供了與此一運用基礎相關之有用資訊，包含應適用之安全維護措

[14] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp 217_en.pdf . Accessed 24 April 2017

第06/2014號意見依據第95/46/EC號指令第7條關於資料控管者正當利益之見解。歐盟執委會，2014年4月9日.http：//ec.europa.eu/justice/data-protection/article- 29 / documentation / opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017年4月24日。

[15] GDPR Recitals 41 and 45.

GDPR前言第41和45點。

[16] Page 19 Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate

施。

4. Article 6(1) (d) – necessary to protect vital interests

第 6 條第 1 項第 d 款 － 為保護重大利益所必須

This covers situations where the processing is necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

此包含當運用為保護當事人或另一自然人生命重要利益所必須之情況。

Certain types of processing may serve important public interest grounds as well as the vital interests of the data subject. Examples of this may include profiling necessary to develop models that predict the spread of life-threatening diseases or in situations of humanitarian emergencies. In these cases, however, and in principle, the controller can only rely on vital interest grounds if no other legal basis for the processing is available.[17] If the processing involves special category personal data the controller would also need to ensure that they meet the requirements of Article 9(2) (c).

某些類型之運用可能係為重要公共利益以及當事人之重大利益。這些情況之示例可能包含當剖析對開發預測威脅生命疾病之模型或人道主義緊急情況為必須時。然而，在這些情況下，原則上，控管者只有在沒有其他適合之運用法律依據時，始得以重要利益為理由。[17]若運用涉及特種個人資料，控管者亦需確保其符合第9條第2項第c款之要求。

5. Article 6(1) (e) – necessary for the performance of a task carried out in the public interest or exercise of official authority

第 6 條第 1 項第 e 款 － 因履行公共利益或行使公權力而執行任務所必須

Article 6(1) (e) might be an appropriate basis for public sector profiling in certain circumstances. The task or function must have a clear basis in law.

在某些情況下，第6條第1項第e款可作為公部門執行剖析之適當基礎。然其任務或職能必須在法律上有明確之基礎。

6. Article 6(1) (f) – necessary for the legitimate interests[18] pursued by the controller or by a third party

第 6 條第 1 項第 f 款 － 為控管者或第三方追求正當利益[18]所必須

---

interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017

第29條個資保護工作小組第19頁。第95/46 / EC號指令第7條關於資料控管者正當利益概念第06/2014號意見。歐盟執委會，2014年4月9日http：//ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017年4月24日。

[17] GDPR Recital 46

GDPR前言第46點。

[18] Legitimate interests listed in GDPR Recital 47 include processing for direct marketing purposes and

Profiling is allowed if it is necessary for the purposes of the legitimate interests[19] pursued by the controller or by a third party. However, Article 6(1) (f) does not automatically apply just because the controller or third party has a legitimate interest. The controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms.

若為控管者或第三方追求正當利益[19]之目的所必須，可執行剖析。然而，第6條第1項第f款並不僅因控管者或第三方擁有正當利益而自動適用。控管者必須進行平衡判斷，以評估其利益是否為當事人利益或基本權利和自由所超越。

The following are particularly relevant:

下述幾點尤為相關：

- the level of detail of the profile (a data subject profiled within a broadly described cohort such as 'people with an interest in English literature', or segmented and targeted on a granular level);
  剖析檔案之詳盡程度（當事人被剖析歸類在某個廣泛描述族群，例如「對英語文學感興趣的人」，或在細度層級進行劃分和目標鎖定）；
- the comprehensiveness of the profile (whether the profile only describes a small aspect of the data subject, or paints a more comprehensive picture);
  剖析檔案之全面性（剖析檔案是否僅描述與當事人相關之一小部分，或是更加全面性的描繪）；
- the impact of the profiling (the effects on the data subject); and
  剖析之影響（對當事人之影響）；及
- the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.
  旨在確保剖析程序之公正、無歧視和正確之安全維護措施。

Although the WP29 opinion on legitimate interests[20] is based on Article 7 of the data protection Directive 95/46/EC (the Directive), it contains examples that are still useful and relevant for controllers carrying out profiling. It also suggests it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across

---

processing strictly necessary for the purposes of preventing fraud.
GDPR前言第47點所列舉之正當利益包含為行銷目的之運用和為防止欺詐之目的而確實必要之運用。

[19] The controller's "legitimate interest" cannot render profiling lawful if the processing falls within the Article 22(1) definition.
若運用屬於第22條第1項之範圍，則控管者之「正當利益」不得作為剖析之合法依據。

multiple websites, locations, devices, services or data-brokering.
儘管WP29關於正當利益[20]之意見係基於第95/46/EC號資料保護指令（指令）第7條，然其涵蓋之示例對於執行剖析之控管者仍有效且相關。該意見亦表明，當控管者為行銷或廣告目的而執行侵入性剖析和追蹤活動時，很難使用正當利益作為合法依據，例如涉及跨越多個網站、位置、設備、服務或資料仲介而追蹤當事人之控管者。

The controller should also consider the future use or combination of profiles when assessing the validity of processing under Article 6(1) (f).
在評估第6條第1項第f款運用之有效性時，控管者亦應考量對剖析檔案未來之使用或組合。

C. Article 9 – Special categories of data
第9條 － 特種資料

Controllers can only process special category personal data if they can meet one of the conditions set out in Article 9(2), as well as a condition from Article 6. This includes special category data derived or inferred from profiling activity.
控管者須符合第9條第2項規定要件之一以及第6條之規定，始可運用特種個資。此包含從剖析活動中衍伸或推論之特種資料。

Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.
剖析可透過資料推論以建立特種資料，這些推論資料本身並非特種資料，然當與其他資料結合時即成為特種資料。例如，可從個人食品購物記錄結合食品質量和能量含量之資料以推論其健康情況。

Correlations may be discovered that indicate something about individuals' health, political convictions, religious beliefs or sexual orientation, as demonstrated by the following example:
關聯性之發現可指出當事人的健康狀況、政治理念、宗教信仰或性取向，如下例所示：

[20] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014, Page 47, examples on pages 59 and 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017
第 29 條個資保護工作小組。第 95/46 / EC 號指令第 7 條關於資料控管者正當利益概念第 06/2014 號意見。歐盟執委會，2014 年 4 月 9 日，第 47 頁，第 59 和 60 頁中之示例 http://ec.europa.eu/justice/data-protection/article-29 / documentation / opinion-recommendation / files / 2014 / wp 217_en.pdf。瀏覽日期： 2017 年 4 月 24 日。

Example

示例

One study[21] combined Facebook 'likes' with limited survey information and found that researchers accurately predicted a male user's sexual orientation 88% of the time; a user's ethnic origin 95% of the time; and whether a user was Christian or Muslim 82% of the time.

一項研究[21]將Facebook的「讚」與有限的調查資訊相結合，發現研究人員準確地預測了88%男性用戶性取向；95%用戶種族來源；82%用戶是基督徒或穆斯林教徒。

If sensitive preferences and characteristics are inferred from profiling, the controller should make sure that:

若從剖析中推論出敏感之個人偏好和特徵，控管者應確保：

- the processing is not incompatible with the original purpose;
  運用與原始目的不會不相容；
- they have identified a lawful basis for the processing of the special category data; and
  確認了運用特種資料之合法依據；及
- they inform the data subject about the processing.
  已就相關運用告知當事人。

Automated decision-making as defined in Article 22(1) that is based on special categories of data is covered in Chapter IV (section D).

第IV章（第D節）涵蓋了第22條第1項所定義之基於特種資料所為之自動化決策。

D. Rights of the data subject[22]
當事人之權利[22]

The GDPR introduces stronger rights for data subjects and creates new obligations for

[21] Michael Kosinski, David Stilwell and Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour. Proceedings of the National Academy of Sciences of the United States of America, http://www.pnas.org/content/110/15/5802.full.pdf . Accessed 29 March 2017.
Michael Kosinski，David Stilwell和Thore Graepel。私人特徵和屬性可從人類行為之數位記錄預測。美國國家科學院會議記錄，http：//www.pnas.org/content/110/15/5802.full.pdf。瀏覽日期： 2017年3月29日。

[22] This Section is relevant for both profiling and automated decision-making. For automated decision making under Article 22, please note that there are also additional requirements as described in Chapter IV.
本章節與剖析和自動化決策相關。對於第22條規定下之自動化決策，請注意第IV章中就此尚有其他要求。

controllers.
GDPR加強了當事人之權利，並對控管者加諸新的義務。

In the context of profiling these rights are actionable against the controller creating the profile and the controller making an automated decision about a data subject (with or without human intervention), if these entities are not the same.
在剖析之背景下，當事人對於建立剖析檔案之控管者和做出關於當事人之自動化決策（無論是否有人為參與）的控管者（若兩者非同一控管者），均得行使權利。

Example
示例

A data broker undertakes profiling of personal data. In line with their Article 13 and 14 obligations the data broker should inform the individual about the processing, including whether they intend to share the profile with any other organisations. The data broker should also present separately details of the right to object under Article 21(1).
資料仲介從事對個人資料之剖析。依據第13條和第14條之義務，資料仲介應就相關運用告知當事人，包括其是否打算與任何其他組織共享該剖析檔案。資料仲介亦應單獨詳列出第21條第1項所規定之拒絕權。

The data broker shares the profile with another company. This company uses the profile to send the individual direct marketing.
資料仲介與另一家公司共享剖析檔案。而該公司使用此檔案對當事人行銷。

The company should inform the individual (Article 14(1) (c)) about the purposes for using this profile, and from what source they obtained the information (14(2) (f)). The company must also advise the data subject about their right to object to processing, including profiling, for direct marketing purposes (Article 21(2)).
該公司應告知當事人（第14條第1項第c款）關於使用剖析檔案之目的，以及從何處獲得此資訊（第14條第2項第f款）。該公司亦須向當事人告知有關拒絕運用(包括為行銷目的之剖析) 之權利（第21條第2項）。

The data broker and the company should allow the data subject the right to access the information used (Article 15) to correct any erroneous information (Article 16), and in certain circumstances erase the profile or personal data used to create it (Article 17). The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed. [23]

資料仲介和公司應允許當事人有權近用其被使用之資訊（第15條）、更正任何錯誤資訊（第16條），並在某些情況下刪除剖析檔案或用以建立該檔案之個人資料（第17條）。另亦應提供當事人其剖析檔案之相關資訊，例如被分置於何種「分類」或「類型」之資訊。[23]

If the company uses the profile as part of a solely automated decision-making process with legal or similarly significant effects on the data subject, the company is the controller subject to the Article 22 provisions. (This does not exclude the data broker from Article 22 if the processing meets the relevant threshold.)

若公司使用該剖析檔案作為純自動化決策程序之一部分，而對當事人產生法律或類似重大之影響時，該公司則屬於受第22條規定拘束之控管者。（若運用符合相關門檻時，亦不排除第22條對資料仲介之適用。）

1. Articles 13 and 14 – Right to be informed
第 13 條和第 14 條 - 被告知權

Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.

鑑於「透明」為GDPR之核心原則，控管者必須確保向當事人清晰且簡單地說明剖析或自動化決策程序之運作。

In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22 provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject.[24]

尤其是，若運用涉及基於剖析而為之決策（無論是否適用第22條之規定），則必須向當事人清楚表明運用之目的是為了（a）剖析及（b）以該剖析檔案而作出決策。[24]

---

[23] The Norwegian Data Protection Authority. The Great Data Race -How commercial utilisation of personal data challenges privacy. Report, November 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data- Race/ Accessed 24 April 2017
挪威資料保護機關。大數據競賽 - 個人資料之商業利用對隱私權之挑戰。報告，2015年11月。https://www.datatilsynet.no/English/Publications/The- Great-Data-Race / 瀏覽日期：2017年4月24日。

[24] GDPR – Article 13(1)(c) and Article 14(1)(c). Article 13(2)(f) and 14(2)(g) require the controller to inform the data subject about the existence of automated decision-making, including profiling, described in Article 22(1) and (4). This is explained further in Chapter IV.
GDPR－ 第13條第1項第c款和第14條第1項第c款。第13條第2項第f款和第14條第2項第g款要求控管者告知當事人有關第22條第1項和第4項所述自動化決策之存在(包含剖析)。將在第IV章對此作進一步說明。

Recital 60 states that giving information about profiling is part of the controller's transparency obligations under Article 5(1) (a). The data subject has a right *to be informed* by the controller about and, in certain circumstances, a right *to object to* 'profiling', *regardless* of whether solely automated individual decision-making based on profiling takes place.

前言第60點指出，提供有關剖析之資訊係控管者依據第5條第1項第a款規定下透明義務之一部分。*無論*是否發生以剖析為基礎之純自動化個人決策，當事人有權*獲得*控管者之*告知*，並在某些情況下，有權*拒絕*「剖析」。

Further guidance on transparency in general is available in the WP29 Guidelines on transparency under the GDPR[25].

WP29關於GDPR之透明化之指引為透明化提供了進一步指導[25]。

2. Article 15 – Right of access

第 15 條 – 近用權

Article 15 gives the data subject the right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile.

第15條規定當事人有權獲得任何用於剖析之個人資料的詳細資訊，包含用於建構剖析檔案之資料類型。

In addition to general information about the processing, pursuant to Article 15(3), the controller has a duty to make available the data used as input to create the profile as well as access to information on the profile and details of which segments the data subject has been placed into.

除了關於運用之一般資訊外，依據第15條第3項，控管者有責任提供用作建立剖析檔案之輸入資料，以及提供對該剖析檔案資訊之近用和當事人被歸入分類之細節。

This differs from the right to data portability under Article 20 where the controller only needs to communicate the data provided by the data subject or observed by the controller and not the profile itself.[26]

此與第20條規定之資料可攜權不同，在第20條中，控管者僅需傳遞由當事人提供或由控管者觀察所得之資料，而不包含剖析檔案本身。[26]

---

[25] Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679 WP260, 28 November 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accessed 18 December 2017.

第29條個資保護工作小組。關於第2016/679號規則之透明化指引(WP260)，2017年11月28日 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850，瀏覽日期：2017年12月18日。

[26] Page 9, WP29 Guidelines on the Right to data portability, WP242 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Accessed 8 January 2018

第9頁，WP29關於資料可攜權指引，WP242。http://ec.europa.eu/newsroom/document.cfm?doc_id=45685。瀏覽日期：2018年1月8日。

Recital 63 provides some protection for controllers concerned about revealing trade secrets or intellectual property, which may be particularly relevant in relation to profiling. It says that the right of access 'should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software'. However, controllers cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information to the data subject.

當剖析與揭露營業秘密或智慧財產權尤為相關時，前言第63點為控管者提供了一些保護。該前言規定，近用權「不應對他人之權利或自由產生不利影響，包含營業秘密或智慧財產權，尤其是保護軟體著作權」。然而，控管者不能以保護其營業秘密作為拒絕近用或拒絕向當事人提供資訊之理由。

Recital 63 also specifies that 'where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.'

前言第63點亦指出「在可能之情況下，控管者應能夠提供對安全系統之遠端存取，而該系統將使當事人能夠直接近用其個人資料。」

3. Article 16 - Right to rectification, Article 17 Right to erasure and Article 18 Right to restriction of processing

第 16 條 － 更正權、第 17 條刪除權和第 18 條限制運用權

Profiling can involve an element of prediction, which increases the risk of inaccuracy. The input data may be inaccurate or irrelevant, or taken out of context. There may be something wrong with the algorithm used to identify correlations.

剖析可能涉及預測因素，因而增加不正確之風險。輸入的資料可能不正確或不相關，或脫離脈絡。而用於識別關聯性之演算法可能存在某些問題。

The Article 16 right to rectification might apply where, for example, an individual is placed into a category that says something about their ability to perform a task, and that profile is based on incorrect information. Individuals may wish to challenge the accuracy of the data used and any grouping or category that has been applied to them.

第16條之更正權可適用於如，當事人就執行任務之能力被分類，然而該剖析檔案所依據之資訊不正確。當事人可能希望對所使用資料之正確性以及所被歸類劃分之任何組別或類型提出異議。

The rights to rectification and erasure[27] apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person).

更正和刪除之權利[27]適用於「輸入之個人資料」（用於建立剖析檔案之個人資料）以及「輸出之資料」（剖析檔案本身或給予當事人之「評分」）。

Article 16 also provides a right for the data subject to complement the personal data with additional information.

第16條亦賦予當事人得以額外資訊補充個人資料之權利。

Example

示例

A local surgery's computer system places an individual into a group that is most likely to get heart disease. This 'profile' is not necessarily inaccurate even if he or she never suffers from heart disease. The profile merely states that he or she is *more likely* to get it. That may be factually correct as a matter of statistics.

一個地區外科電腦系統將某當事人歸類於最容易罹患心臟病之群體中。即使該當事人從未患有心臟病，此種「剖析」也不一定不正確。該檔案僅指出其更*有可能*罹患心臟病。就統計而言，此歸類可能事實上是正確的。

Nevertheless, the data subject has the right, taking into account the purpose of the processing, to provide a supplementary statement. In the above scenario, this could be based, for example, on a more advanced medical computer system (and statistical model) factoring in additional data and carrying out more detailed examinations than the one at the local surgery with more limited capabilities.

然而，當事人有權利在考量運用目的之情況下提供補充聲明。在上述情境中，其可依據如更先進之醫學電腦系統（和統計模型），納入其他資料，並進行比能力有限的地區外科更詳盡之檢查。

The right to restrict processing (Article 18) will apply to any stage of the profiling process.

限制運用之權利（第18條）將適用於剖析程序中之任何階段。

4. Article 21 – Right to object

第 21 條 － 拒絕權

The controller has to bring details of the right to object under Article 21(1) and (2) *explicitly* to the data subject's attention, and present it clearly and separately from other information (Article 21(4)).

[27] GDPR – Article 17[28] GDPR- Article 18(1)(d).
GDPR － 第 17 條 GDPR － 第 18 條第 1 項第 d 款。

控管者必須*清楚地*使當事人注意到第21條第1項和第2項所規定拒絕權之細節，並將其與其他資訊明確且分開呈現（第21條第4項）。

Under Article 21(1) the data subject can object to processing (including profiling), on grounds relating to his or her particular situation. Controllers are specifically required to provide for this right in all cases where processing is based on Article 6(1) (e) or (f).
依據第21條第1項，當事人可因與其相關之特定情況而拒絕運用（包含剖析）。當運用係依據第6條第1項第e款或f款之所有情況下，特別要求控管者提供此項權利。

Once the data subject exercises this right, the controller must interrupt[28] (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject. The controller may also have to erase the relevant personal data.[29]
一旦當事人行使此項權利，控管者就必須中斷[28]（或避免啟動）剖析程序，除非其可提出具說服性之正當理由超越當事人之利益、權利和自由。控管者可能亦須刪除相關個人資料。[29]

The GDPR does not provide any explanation of what would be considered compelling legitimate grounds. [30] It may be the case that, for example, the profiling is beneficial for society at large (or the wider community) and not just the business interests of the controller, such as profiling to predict the spread of contagious diseases.
GDPR並無提供任何有關具說服性正當理由之說明。[30]可能之情況為，例如，剖析有益於整個社會（或更廣泛之社群），而不僅係控管者之商業利益，例如預測傳染病蔓延之剖析。

The controller would need to:
控管者可能必須：

- consider the importance of the profiling to their particular objective;
  考量剖析對其特定目的之重要性;

---

[28] GDPR- Article 18(1)(d).
GDPR - 第18條第1項第d款。
[29] GDPR – Article 17(1)(c).
GDPR - 第17條第1第c款。
[30] See explanation on legitimacy, Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 9 April 2014. Page 24 - 26 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accessed 24 April 2017
請參正當性之說明，第29條個資保護工作小組第95/46/EC號指令第7條關於資料控管者之正當利益概念第06/2014號意見。2014年4月9日。第24－26頁 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommended / files / 2014 / wp217_en.pdf。瀏覽日期： 2017年4月24日。

- consider the impact of the profiling on the data subject's interest, rights and freedoms – this should be limited to the minimum necessary to meet the objective; and
  考量剖析對當事人利益、權利和自由之影響 – 此應限於為達到目的所需之最小程度；及
- carry out a balancing exercise.
  進行平衡使用。

There must always be a balancing exercise between the competing interests of the controller and the basis for the data subject's objection (which may be for personal, social or professional reasons). Unlike in the Directive 95/46/EC, the burden of proof to show compelling legitimate grounds lies with the controller rather than the data subject.
在控管者的競爭利益和當事人的拒絕權利基礎（此可能是基於個人、社會或專業原因）間必須始終存在一種平衡判斷。不同於第95/46/EC號指令，提供具說服力正當理由之舉證責任在於控管者而非當事人。

It is clear from the wording of Article 21 that the balancing test is different from that found in Article 6(1)(f). In other words, it is not sufficient for a controller to just demonstrate that their earlier legitimate interest analysis was correct. This balancing test requires the legitimate interest to be *compellin*g, implying a higher threshold for overriding objections.
從第21條的措辭可清楚地看出，平衡測試與第6條第1項第f款之規定不同。易言之，若控管者僅提出其先前正當利益分析為正確並不足夠。此種平衡測試要求正當利益具*說服力*，此意味著若要推翻拒絕權須符合更高之門檻。

Article 21(2) grants an *unconditional* right for the data subject to object to the processing of their personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.[31] This means that there is no need for any balancing of interests; the controller must respect the individual's wishes without questioning the reasons for the objection. Recital 70 provides additional context to this right and says that it may be exercised at any time and free of charge.
第21條第2項賦予當事人得*無條件*拒絕為行銷目的運用其個人資料之權利，包含與此類行銷相關之剖析[31]。此意味著不需進行任何利益平衡判斷；控管者必須尊重當事人意願，而

[31] In line with Article 12(2) controllers who collect personal data from individuals with the aim of using it for direct marketing purposes should, at the moment of collection, consider offering data subjects an easy way to indicate that they do not wish their personal data to be used for direct marketing purposes, rather than requiring them to exercise their right to object at a later occasion.
依據第12條第2項，當控管者基於行銷目的而由當事人處蒐集個人資料，在蒐集資料同時，應考量提供當事人便捷之方式以表明不希望個人資料被使用於行銷之目的，而非要求當事人於其後之時點行使拒絕權。

不得質疑拒絕之理由。前言第70點為拒絕權提供了額外之背景，並表示可在任何時間無償行使該權利。

IV. Specific provisions on solely automated decision- making as defined in Article 22
第22條所定義之純自動化決策之具體規定

Article 22(1) says
第22條第1項規定

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces *legal effects* concerning him or her or *similarly significantly affects him or her*.
> 對當事人產生*法律效果*或*類似重大影響*之純自動化決策（包含剖析），當事人有不受拘束的權利。

The term "right" in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data.
該條款中「權利」一詞並不意味著第22條第1項僅適用於當事人主動行使之情況。第22條第1項針對純粹基於自動化運用之決策，建立了一般性的禁止原則。此種禁止之適用無關當事人是否對其個人資料之運用採取行動。

In summary, Article 22 provides that:
綜上所述，第22條規定：

(i) as a rule, there is a general prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect;
作為原則規範，當決策可產生法律或類似重大之影響時，通常禁止完全自動化的個人決策（包含剖析）；

(ii) there are exceptions to the rule;
該原則規範具有例外;

(iii) where one of these exceptions applies, there must be measures in place to safeguard the data subject's rights and freedoms and legitimate interests[32].
若適用其中一項例外情形，則必須採取安全維護措施確保當事人之權利和自由以

及正當利益[32]。

This interpretation reinforces the idea of the data subject having control over their personal data, which is in line with the fundamental principles of the GDPR. Interpreting Article 22 as a prohibition rather than a right to be invoked means that individuals are automatically protected from the potential effects this type of processing may have. The wording of the Article suggests that this is the intention and is supported by Recital 71 which says:
此種解釋強化了當事人得控制其個人資料之概念，此亦符合GDPR之基本原則。將第22條解釋為禁止而非被行使之權利，意味著當事人就此類運用可能產生之潛在影響會自動受到保護。該條文之措辭表明此一意圖，而前言第71點亦加以支持，並指出：

> However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law……, or necessary for the entering or performance of a contract……., or when the data subject has given his or her explicit consent
> 然而，在歐盟或成員國法律明確授權之情況下.....或為簽訂或履行契約所必須.....或當事人給予明確同意時，應允許基於此種運用所為之決策（包含剖析）。

This implies that processing under Article 22(1) is not allowed generally.[33]
此意味著原則不允許依據第22條第1項所為之運用。[33]

However the Article 22(1) prohibition *only* applies in specific circumstances when a decision based solely on automated processing, including profiling, has a legal effect on or similarly significantly affects someone, as explained further in the guidelines. Even in these cases there are defined exceptions which allow such processing to take place.
然而，如本指引進一步之解釋，第22條第1項之禁止*僅*適用於特定情況，即當基於純自動運用之決策（包含剖析）對當事人產生法律效果或類似重大影響時。即使在這些情況下，亦存在允許進行此類運用之明確例外情形。

The required safeguarding measures, discussed in more detail below, include the right to be informed (addressed in Articles 13 and 14 – specifically meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), and

[32] Recital 71 says that such processing should be "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."
前言第71點表示，此類運用應「基於適當安全維護措施，其中應包含當事人之具體資訊以及取得人為參與、表達觀點、取得評估後所作決策之理由、和質疑該決策之權利。」

[33] Further comments on the interpretation of Article 22 as a prohibition can be found in Annex 2.
關於第22條作為禁止規則解釋之進一步評論請參閱附錄2。

safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)).

下文將詳細討論所需之安全維護措施，包含被告知之權利（規定於第13條和第14條 － 尤其是關於所涉邏輯之有意義資訊，以及對當事人之重要性及預設之後果）及安全維護措施，例如取得人為參與之權利和對決策提出異議之權利（規定於第22條第3項）。

Any processing likely to result in a high risk to data subjects requires the controller to carry out a Data Protection Impact Assessment (DPIA).[34] As well as addressing any other risks connected with the processing, a DPIA can be particularly useful for controllers who are unsure whether their proposed activities will fall within the Article 22(1) definition, and, if allowed by an identified exception, what safeguarding measures must be applied.

任何可能造成當事人高風險之運用皆要求控管者辦理個資保護影響評估（DPIA）。[34]除可因應與運用相關之任何其他風險外，對不確定所擬活動是否屬於第22條第1項之定義範圍，或當該活動屬於明確例外情形時應採取何種安全維護措施，DPIA尤其可提供控管者協助。

A ‘Decision based solely on automated processing’ 「基於純自動化運用之決策」

Article 22(1) refers to decisions ‘based solely’ on automated processing. This means that there is no human involvement in the decision process.

第22條第1項係指「純基於」自動化運用之決策。此意味著決策程序中並無人為參與。

Example

示例

An automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be ‘based solely’ on automated processing.

自動化程序可產生實際上與當事人相關之建議。若在做出最終決策時有人為審查並考量其他因素，則該決策並非「純基於」自動化運用。

[34] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.4 April 2017. European Commission. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.
2017年4月4日歐盟執委會29條資料保護工作小組發佈第2016/679號規則關於個資保護影響評估指引（DPIA）以及確認運用是否「可能造成高風險」。http://ec.europa.eu/newsroom/document.cfm?doc_id=44137，瀏覽日期：2017年4月24日。

The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing.

控管者無法透過編造人為參與以規避第22條之規定。例如，若透過人為例行將自動化生成之剖析檔案應用於當事人，而對結果並無任何實際影響，則此仍屬於是純基於自動化運用之決策。

To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.

為符合有效之人為參與，控管者必須確保對決策之任何監督皆具有意義，而非僅為一種象徵性之行為。該參與應由具有改變決策權限和能力之人執行。參與人應考量所有相關資料，以作為分析之一部分。

As part of their DPIA, the controller should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place.

作為DPIA的一部分，控管者應識別並記錄人為參與決策程序之程度以及其所發生之階段。

B ‘Legal’ or ‘similarly significant’ effects
「法律」或「類似重大」之影響

The GDPR recognises that automated decision-making, including profiling can have serious consequences for individuals. The GDPR does not define ‘legal’ or ‘similarly significant’ however the wording makes it clear that only serious impactful effects will be covered by Article 22.

GDPR認識到自動化決策（包含剖析）可能會對當事人造成嚴重後果。GDPR並無定義何謂「法律」或「類似重大」，然此措辭明確指出第22條僅涵蓋重大之影響。

‘Decision producing legal effects’
「產生法律效果之決策」

A legal effect requires that the decision, which is based on solely automated processing, affects someone’s legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person’s legal status or their rights under a contract. Examples of this type of effect include automated decisions about an individual

that result in:
法律效果是指基於純自動化運用之決策對某人之合法權利產生影響，例如與他人交流、選舉投票或採取法律行動之自由。其亦可能影響某人之合法地位或於契約下之權利。此類影響之示例包含對當事人之自動化決策導致：

- cancellation of a contract;
  解除契約；
- entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit;
  享有或拒絕法律賦予之特定社會福利之權利，例如子女或住房福利；
- refused admission to a country or denial of citizenship.
  拒絕進入某個國家或拒絕公民身份。

‘Similarly significantly affects him or her’
「對當事人造成類似重大之影響」

Even if a decision-making process does not have an effect on people’s legal rights it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly significant in its impact.
即使決策程序並未對當事人之法律權利產生任何效果，然若產生之效果等同於法律效果或有類似重大之影響時，仍屬於第22條之範圍。

In other words, even where there is no change in their legal rights or obligations, the data subject could still be impacted sufficiently to require the protections under this provision. The GDPR introduces the word ‘similarly’ (not present in Article 15 of Directive 95/46/EC) to the phrase ‘significantly affects’. Therefore the threshold for *significance* must be similar to that of a decision producing a legal effect.
易言之，即使其法定權利或義務並無發生變化，當事人仍可因受到重大影響，而需要該條款所提供之保護。GDPR引進「類似」一詞（第95/46 / EC號指令第15條中並無此規定）來修飾「重大影響」。因此，*重大性*之門檻必須類似於產生法律效果之決策。

Recital 71 provides the following typical examples: ‘automatic refusal of an online credit application’ or ‘e-recruiting practices without any human intervention’.
前言第71點提供了以下典型示例：「自動拒絕網路信用申請」或「無人為參與之網路招募活動」。

For data processing to significantly affect someone the effects of the processing must be

sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:
當資料運用對某人產生重大影響時，運用之效果必須足夠重大或重要到值得引起注意。易言之，決策必須可能：

- significantly affect the circumstances, behaviour or choices of the individuals concerned;
  重大影響相關個人之情況、行為或選擇；
- have a prolonged or permanent impact on the data subject; or
  對當事人產生長期或永久之影響；或
- at its most extreme, lead to the exclusion or discrimination of individuals.
  在極端情況下，造成對個人之排斥或歧視。

It is difficult to be precise about what would be considered sufficiently *significant* to meet the threshold, although the following decisions could fall into this category:
雖然下列決策可能屬於此一類型，但很難準確認定何種情況可被認定為足夠重大以符合門檻：

- decisions that affect someone's financial circumstances, such as their eligibility to credit;
  影響某人財務情況之決策，例如獲得信貸之資格；
- decisions that affect someone's access to health services;
  影響某人獲得醫療服務之決策；
- decisions that deny someone an employment opportunity or put them at a serious disadvantage;
  剝奪某人就業機會或使其處於嚴重劣勢之決策；
- decisions that affect someone's access to education, for example university admissions.
  影響某人接受教育之決策，例如大學錄取。

This bring us also to the issue of online advertising, which increasingly relies on automated tools and involves solely automated individual decision-making. As well as complying with the general provisions of the GDPR, covered in Chapter III, the provisions of the proposed ePrivacy Regulation may also be relevant. Furthermore, children require enhanced protection, as will be discussed below in Chapter V.
此亦顯現了網路廣告的問題，網路廣告越來越依賴於自動化工具，且涉及純自動化之個人決策。除了需遵守第III章所述GDPR之一般規定外，草擬之數位隱私規則之規定亦與此處相關聯。此外，如下文第V章中所述，對兒童需加強保護。

In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'.
在許多典型情況下，基於剖析而呈現目標式廣告之決策不會對個人造成類似重大影響，例如基於簡單人口統計檔案所為之主流網路時尚商店廣告：「布魯塞爾地區25至35歲女性可能對時尚和某些服飾產品感興趣」。

However it is possible that it may do, depending upon the particular characteristics of the case, including:
然而，依據個案具體特性，廣告可能有類似重大影響，包含：

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
  剖析程序之侵入性，包含跨越多個網站、設備和服務追蹤個人；
- the expectations and wishes of the individuals concerned;
  相關個人之期待和願望；
- the way the advert is delivered; or
  廣告之投放方式；或
- using knowledge of the vulnerabilities of the data subjects targeted.
  利用對目標當事人弱點之了解。

Processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults. For example, someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt.
對一般個人影響不大之運用實際上可能對某些社會族群產生重大影響，例如少數族群或易受傷害之成年人。例如，已知或可能陷入財務困境之人經常是高利息貸款廣告的目標，且可能會簽訂這些契約並產生進一步之債務。

Automated decision-making that results in differential pricing based on personal data or personal characteristics could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.
依據個人資料或個人特性造成差別定價之自動化決策亦可能產生重大影響，例如以過高之價格有效地阻止某人取得某些商品或服務。

Similarly significant effects could also be triggered by the actions of individuals other than the

one to which the automated decision relates. An illustration of this is given below.
類似重大影響亦可能並非來自於相關自動化決策而是因個人之行為所觸發。以下示例說明了此種情況。

Example
示例

Hypothetically, a credit card company might reduce a customer's card limit, based not on that customer's own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores.
假設信用卡公司可能並非基於客戶的還款歷史而降低其信用卡之限額，而是基於非傳統的信用標準，例如對居住於同一區域和消費於同一商店之其他客戶的分析。

This could mean that someone is deprived of opportunities based on the actions of others.
此意味著某人可能基於他人之行為而被剝奪了機會。

In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.
在不同脈絡下，使用此類特性之優勢在於可將信用擴展至沒有傳統信用記錄且可能遭受拒絕之人。

C Exceptions from the prohibition
禁止之例外情形

Article 22(1) sets out a general prohibition on solely automated individual decision-making with legal or similarly significant effects, as described above.
如上所述，第22條第1項規定了造成法律或類似重大影響之純自動化個人決策的一般性禁止原則。

This means that the controller should not undertake the processing described in Article 22(1) unless one of the following Article 22(2) exceptions applies - where the decision is:
此意味著控管者不應執行第22條第1項所述之運用，除非適用下列第22條第2項之例外情形 – 當決策係：

(a) necessary for the performance of or entering into a contract;
履行或簽訂契約所必須；

(b) authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
控管者依歐盟或成員國法律之授權所為，且該法律規定了保護當事人權利和自由以及正當利益之適當安全維護措施；或

(c) based on the data subject's explicit consent.
基於當事人之明確同意。

Where the decision-making involves special categories of data defined in Article 9(1) the controller must also ensure that they can meet the requirements of Article 22(4).
若決策涉及第9條第1項規定之特種資料，則控管者亦須確保能夠滿足第22條第4項之要求。

1. Performance of a contract
履行契約

Controllers may wish to use solely automated decision-making processes for contractual purposes because they believe it is the most appropriate way to achieve the objective. Routine human involvement can sometimes be impractical or impossible due to the sheer quantity of data being processed.
基於契約目的，控管者可能希望使用純自動化決策程序，因其認為此為實現目標最合適之方式。由於運用資料數量龐大，例行的人為參與有時可能是不切實際或不可能的。

The controller must be able to show that this type of processing is necessary, taking into account whether a less privacy-intrusive method could be adopted. [35] If other effective and less intrusive means to achieve the same goal exist, then it would not be 'necessary'.
控管者必須能夠證明此種類型之運用是必要的，同時考量是否得採用較少侵入隱私之方式。[35]若存在可實現相同目的之其他有效且較少侵入性之方式，則該運用就並非係「必要的」。

[35] Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. AToolkit European Data Protection Supervisor, 11 April 2017, https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf Accessed 24 April 2017
Buttarelli，Giovanni。「限制保護個人資料基本權利措施之必要性評估」。歐盟資料保護監管人工具包，2017

Automated decision-making described in Article 22(1) may also be necessary for pre-contractual processing.

第22條第1項所述之自動化決策對於契約簽訂前之(資料)運用亦可能有其必要。

Example

示例

A business advertises an open position. As working for the business in question is popular, the business receives tens of thousands of applications. Due to the exceptionally high volume of applications, the business may find that it is not practically possible to identify fitting candidates without first using fully automated means to sift out irrelevant applications. In this case, automated decision-making may be necessary in order to make a short list of possible candidates, with the intention of entering into a contract with a data subject.

一家企業宣傳一個職位空缺。由於為此企業工作相當受到歡迎，該企業收到了數以萬計的申請表。由於申請表數量異常龐大，企業可能會發現，若無事先使用純自動方式篩選掉不相關之申請表，要確定合適之候選人實際上是不可能的。在此情形下，為列出較短的可能候選人名單，以便與當事人簽訂契約，自動化決策可能是必須的。

Chapter III (Section B) provides more information on contracts as a lawful basis for processing.

第III章（第B節）提供了更多有關以契約作為運用合法依據之資訊。

2. Authorised by Union or Member State law

經歐盟或成員國法律授權

Automated decision-making including profiling could potentially take place under 22(2)(b) if Union or Member State law authorised its use. The relevant law must also lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

若經歐盟或成員國法律授權，自動化決策（包含剖析）可能得依第22條第2項第b款執行。相關法律亦須制定適當措施以維護當事人之權利和自由以及正當利益。

Recital 71 says that this could include the use of automated decision-making defined in Article 22(1) for monitoring and preventing fraud and tax-evasion, or to ensure the security and reliability of a service provided by the controller.

前言第71點指出，這可能包括使用第22條第1項中所定義之自動化決策來監控和防止詐欺及逃稅，或確保控管者所提供服務之安全性和可靠性。

年4月11日，https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf，瀏覽日期：2017年4月24日。

3. Explicit consent
明確之同意

Article 22 requires explicit consent. Processing that falls within the definition of Article 22(1) poses significant data protection risks and a high level of individual control over personal data is therefore deemed appropriate.
第22條要求明確之同意。屬於第22條第1項定義範圍內之運用，具有重大的資料保護風險，因此當事人對其個人資料之高度控制被認為是適當的。

'Explicit consent' is not defined in the GDPR. The WP29 guidelines on consent[36] provide guidance on how this should be interpreted.
GDPR並未定義何謂「明確之同意」。WP29關於同意之指引[36]就如何解釋此一概念提供了指導。

Chapter III (Section B) provides more information on consent generally.
第III章（第B節）提供了有關同意之更多一般資訊。

D. Special categories of personal data – Article 22(4)
特種個人資料 - 第22條第4項

Automated decision-making (described in Article 22(1)) that involves special categories of personal data is only allowed under the following cumulative conditions (Article 22(4)):
涉及特種個人資料之自動化決策（如第22條第1項所述）僅於符合以下累進條件（第22條第4項）時得執行之：

- there is an applicable Article 22(2) exemption; and
  適用第22條第2項之例外情形；及
- point (a) or (g) of Article 9(2) applies.
  適用第9條第2項第a或g款。

> 9(2) (a) - the explicit consent of the data subject; or
> 第9條第2項第a款 － 當事人明確同意；或

[36] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679 WP259. 28 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accessed 18 December 2017
29條個資保護工作小組。第2016/679號規則（WP259）關於同意之指引。2017年11月28日，http：//ec.europa.eu/newsroom/just/document.cfm？doc_id = 48499。瀏覽日期：2017年12月18日。

9(2) (g) - processing necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
第9條第2項第g款 - 基於歐盟或成員國法律為實現重大公共利益所必須之運用，該法律與所追求之目標應符合比例原則、尊重資料保護權之本質、並提供適當和具體之措施，以維護當事人之基本權利和利益。

In both of the above cases, the controller must put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
在上述兩種情況下，控管者必須採取適當措施以維護當事人之權利和自由以及正當利益。

E Right of data subject[37]
當事人之權利[37]

1. Articles 13(2) (f) and 14(2) (g) - Right to be informed
第 13 條第 2 項第 f 款和 14 條第 2 項第 g 款 － 被告知權

Given the potential risks and interference that profiling caught by Article 22 poses to the rights of data subjects, data controllers should be particularly mindful of their transparency obligations.
鑑於第22條所涉及之剖析對當事人權利構成之潛在風險和干預，資料控管者應特別注意其透明化之義務。

Articles 13(2) (f) and 14(2) (g) require controllers to provide specific, easily accessible information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects.[38]
第13第2項第f款和14條第2項第g款要求控管者就純自動化運用（包含剖析）而為之自動化決策，在造成法律或類似重大影響時，提供明確且易於取得之資訊。[38]

If the controller is making automated decisions as described in Article 22(1), they must:
若控管者執行如第22條第1項所述之自動化決策時，必須：

- tell the data subject that they are engaging in this type of activity;

[37] GDPR Article 12 provides for the modalities applicable for the exercise of the data subject's rights.
GDPR第12條規定了適用於行使當事人權利之方式。
[38] Referred to in Article 22(1) and (4). The WP Guidelines on transparency cover the general information requirements set out in Articles 13 and 14.
於第22條第1項和第4項中提及。WP關於透明化之指引涵蓋了第13條和第14條中規定之一般資訊要求。

告知當事人其正在參與此類活動；

- provide meaningful information about the logic involved; and
  提供有關所涉邏輯之有意義資訊；及
- explain the significance and envisaged consequences of the processing.
  解釋運用之重要性和預設之後果。

Providing this information will also help controllers ensure they are meeting some of the required safeguards referred to in Article 22(3) and Recital 71.
提供這些資訊亦將有助於控管者確保其滿足第22條第3項和前言第71點中提及之某些必要安全維護措施。

If the automated decision-making and profiling does not meet the Article 22(1) definition it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair,[39] and meet all the other information requirements of Articles 13 and 14.
若自動化決策和剖析不符合第22條第1項之定義，提供上述資訊亦屬一種優良實務做法。無論如何，控管者必須向當事人提供足夠之資訊以確保運用之公正性，[39]並滿足第13條和第14條下所有其他資訊之要求。

Meaningful information about the 'logic involved'
有關「所涉邏輯」之有意義資訊

The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works.
機器學習的成長和複雜性使得理解自動化決策程序或剖析之運作變得具有挑戰性。

The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm.[40] The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.
控管者應以簡單之方式告知當事人背後之基本原理，或達成決策時所依據之標準。GDPR

[39] GDPR Recital 60 "The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore the data subject should be informed of the existence of profiling and the consequences of such profiling."
GDPR 前言第60點「控管者應為當事人提供任何必要之進一步資訊，以確保運用之公正性和透明化，同時考量到運用個人資料之具體情況和背景。此外，應告知當事人剖析之存在以及該剖析之後果。」

要求控管者提供有關所涉邏輯之有意義資訊，但並非是所使用演算法之複雜解釋或完整演算法之揭露。[40]然而，提供之資訊應足夠全面，以使當事人了解所作決策之理由。

Example

示例

A controller uses credit scoring to assess and reject an individual's loan application. The score may have been provided by a credit reference agency, or calculated directly based on information held by the controller.

控管者使用信用評分以評估和拒絕當事人之貸款申請。此評分可能是由信貸諮詢機構提供，或直接依據控管者擁有之資訊加以計算。

Regardless of the source (and information on the source must be provided to the data subject under Article 14 (2) (f) where the personal data have not been obtained from the data subject), if the controller is reliant upon this score it must be able to explain it and the rationale, to the data subject.

無論其來源為何（當個人資料並非由當事人處獲得時，則必須依據第14條第2項第f款向當事人提供有關資料來源之資訊），若控管者依賴此評分，則必須能夠向當事人解釋該評分和其基本理由。

The controller explains that this process helps them make fair and responsible lending decisions. It provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

控管者解釋此程序有助於做出公正和負責任之貸款決策。該控管者提供了在做出決策時所考量主要特徵之詳細資訊、此資訊之來源和關聯性。可能包括，例如：

- the information provided by the data subject on the application form;
  申請表上當事人提供之資訊；
- information about previous account conduct , including any payment arrears; and
  有關先前帳戶行為之資訊，包括任何拖欠付款；及
- official public records information such as fraud record information and insolvency records.

[40] Complexity is no excuse for failing to provide information to the data subject. Recital 58 states that the principle of transparency is "of particular relevance in situations where the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him are being collected, such as in the case of online advertising".

複雜性不得作為無法向當事人提供資訊之理由。前言第58點指出，透明化原則「特別適用於當行為者激增以及活動之技術複雜性使當事人難以知曉和了解與其相關之個人資料是由誰以及以何種目的被蒐集，例如網路廣告」。

官方公開記錄資訊，如詐欺記錄資訊和破產記錄。

The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased.
控管者提供之資訊亦包括告知當事人所使用之信用評分方法經定期測試，以確保程序維持公正、有效和無偏見的。

The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).
依據第22條第3項之規定，控管者提供當事人聯繫細節，以便當事人要求重新考量任何拒絕之決策。

‘Significance’ and ‘envisaged consequences’
「重要性」及「預設之後果」

This term suggests that information must be provided about intended or future processing, and how the automated decision-making might affect the data subject.[41] In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given.
此措辭表明必須提供有關預期或未來運用之資訊，以及自動化決策可能如何影響當事人。[41]為了使這些資訊有意義且可理解，應提供可能影響類型之真實、確切之示例。

In a digital context, controllers might be able to use additional tools to help illustrate such effects.
在數位環境中，控管者也許得使用額外工具以協助說明這些影響。

---

[41] Council of Europe. Draft Explanatory Report on the modernised version of CoE Convention 108, paragraph 75: “Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated-decision making including profiling. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a ‘yes’ or ‘no’ decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority.”
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2 . Accessed 24 April 2017
歐盟理事會。歐盟理事會公約 108 現代化版本之解釋性報告草案第 75 段：「當事人應有權了解運用其資料之原因，包括此種原因之後果，以及從而得出之任何結論，尤其是涉及使用演算法進行自動化決策（包含剖析）之案例。例如，在信用評分之情況下，當事人應有權了解支持相關資料運用以及導致「是」或「否」決策之邏輯，而不僅僅是決策本身之資訊。若不能了解這些要素，則無法有效地行使其他實質的安全維護措施，例如拒絕權及向權責機關提出申訴之權利。」
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2。瀏覽日期：2017 年 4 月 24 日。

Example

示例

An insurance company uses an automated decision making process to set motor insurance premiums based on monitoring customers' driving behaviour. To illustrate the significance and envisaged consequences of the processing it explains that dangerous driving may result in higher insurance payments and provides an app comparing fictional drivers, including one with dangerous driving habits such as fast acceleration and last-minute braking.

一間保險公司使用自動化決策程序，以監控客戶之駕駛行為來設定汽車保險費用。為了說明運用之重要性和預設之後果，該公司解釋了危險駕駛可能導致更高的保險金支付，並提供應用程式可與虛擬之駕駛人相比較，包括一位有危險駕駛習慣，如快速加速和緊急煞車之駕駛人。

It uses graphics to give tips on how to improve these habits and consequently how to lower insurance premiums.

該公司使用圖表以提供有關如何改善這些習慣，以及結果將如何降低保險費之建議。

Controllers can use similar visual techniques to explain how a past decision has been made.

控管者可以使用類似之視覺技術以解釋過去決策如何做成。

2. Article 15(1) (h) - Right of access

第 15 條第 1 項第 h 款 – 近用權

Article 15(1) (h) entitles data subjects to have the same information about solely automated decision- making, including profiling, as required under Articles 13(2) (f) and 14(2) (g), namely:

第15條第1項第h款規定，當事人有權依據第13條第2項第f款和14條第2項第g款之規定，取得有關純自動化決策（包含剖析）之相同資訊，即：

- the existence of automated decision making, including profiling;
  自動化決策（包含剖析）之存在；
- meaningful information about the logic involved; and
  有關所涉邏輯之有意義資訊；及
- the significance and envisaged consequences of such processing for the data subject.
  此類運用對當事人之重要性和預設之後果。

The controller should have already given the data subject this information in line with their Article 13 obligations.[42]

控管者應已經依據第13條之義務向當事人提供了這些資訊。[42]

Article 15(1)(h) says that the controller should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision. Recital 63 clarifies this by stating that every data subject should have the right of access to obtain 'communication' about automatic data processing, including the logic involved, and at least when based on profiling, the consequences of such processing,
第15條第1項第h款規定，控管者應向當事人提供有關運用的預設後果之資訊，而非對特定決策之解釋。前言第63點闡明每位當事人應有近用權以獲得有關自動化資料運用之「溝通」，包括所涉之邏輯，且至少在基於剖析之情況下，此種運用之後果。

By exercising their Article 15 rights, the data subject can become aware of a decision made concerning him or her, including one based on profiling.
透過行使第15條之權利，當事人可了解與其相關之決策，包括基於剖析之決策。

The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision.
控管者應向當事人提供可協助其質疑決策之一般資訊（尤其是關於決策程序中考量之因素，以及總體程度上各個因素所佔之「權重」）。

F. Establishing appropriate safeguards
建立適當安全維護措施

If the basis for processing is 22(2)(a) or 22(2)(c), Article 22(3) requires controllers to implement suitable measures to safeguard data subjects' rights, freedoms and legitimate interests. Under Article 22(2)(b) the Member or Union State law that authorises the processing must also incorporate appropriate safeguarding measures.
若運用係基於第22條第2項第a款或第22條第2項第c款，第22條第3項要求控管者採取適當措施以維護當事人之權利、自由及正當利益。依據第22條第2項第b款，由成員國或歐盟法律授權之運用亦須納入適當之安全維護措施。

Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision.
這些措施應至少包括當事人可取得人為參與、表達其觀點、並對決策提出異議之方式。

[42] GDPR Article 12(3) clarifies the timescales for providing this information.
GDPR第12條第3項闡明了提供此類資訊之時間表。

Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject.
人為參與是一項關鍵要素。任何審核必須由具有適當權限和能力改變決策之人員執行。審核人員應對所有相關資料進行全面性評估，包括當事人所提供之任何其他資訊。

Recital 71 highlights that *in any case* suitable safeguards should also include:
前言第71點強調，*在任何情況下*，適當安全維護措施亦應包括：

> .. specific information to the data subject and the right …… to obtain an explanation of the decision reached after such assessment and to challenge the decision.
> …有關當事人之具體資訊和其權利.....以取得對此類評估所達成決策之解釋，並質疑該決策。

The controller must provide a simple way for the data subject to exercise these rights.
控管者必須為當事人提供一種簡單行使這些權利之方式。

This emphasises the need for transparency about the processing. The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis. Transparency requirements are discussed in Chapter IV (section E).
此處強調了對運用透明化之要求。當事人只有在完全瞭解決策如何做成及其依據為何之基礎上，才能對該決策提出質疑或表達其觀點。透明化之要求在第IV章（第E節）中詳加討論。

Errors or bias in collected or shared data or an error or bias in the automated decision-making process can result in:
蒐集或共享資料中之錯誤或偏差，或自動化決策程序中之錯誤或偏差可能導致：

- incorrect classifications; and
  不正確之分類；及
- assessments based on imprecise projections; that
  基於不精確預測之評估；造成
- impact negatively on individuals.
  對個人負面之影響。

Controllers should carry out frequent assessments on the data sets they process to check for any

bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations. Systems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling are other useful measures.
控管者應對其運用之資料集進行經常性評估，以檢驗是否存在偏差，並建立解決任何偏見因素之方法，包括任何對關聯性的過度依賴。其他可用措施包括審核演算法和定期審查自動化決策（包含剖析）之準確性及關聯性的系統。

Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies[43] or discrimination on the basis of special category data. These measures should be used on a cyclical basis; not only at the design stage, but also continuously, as the profiling is applied to individuals. The outcome of such testing should feed back into the system design.
控管者應使用適當之程序和措施，以防止基於特種類型資料之錯誤、不正確[43]或歧視。這些措施應在周期性基礎上使用；不僅於設計階段，且應在其後剖析應用於個人階段時不間斷地使用。相關測試之結果應向系統設計回饋。

Further examples of appropriate safeguards can be found in the Recommendations section。
有關適當安全維護措施之更多示例，請參閱附錄1「建議」。

V. Children and profiling
兒童和剖析

The GDPR creates additional obligations for data controllers when they are processing children's personal data.
GDPR在運用兒童之個人資料時為資料控管者規範了額外之義務。

Article 22 itself makes no distinction as to whether the processing concerns adults or children. However, recital 71 says that solely automated decision-making, including profiling, with legal or similarly significant effects should not apply to children.[44] Given that this wording is not reflected in the Article itself, WP29 does not consider that this represents an absolute prohibition on this type of processing in relation to children. However, in the light of this recital, WP29

[43] GDPR Recital 71 says that:
GDPR 前言第 71 點表示：
"In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised,…."
「為了確保對當事人之公正和透明化運用，考量到運用個人資料之具體情況和背景，控管者應使用適當之數學或統計程序進行剖析，採行適當技術性和組織性措施，以特別確保改正導致個人資料不正確之因素，並儘量減少錯誤之風險，…」

recommends that, as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it.

第22條本身並未就運用是否涉及成人或兒童而加以區分。然而，前言第71點表示，具有法律或類似重大影響之純自動化決策（包含剖析）不應適用於兒童。[44]鑑於此一措辭並未反映於該條文本身，WP29並不認為因此絕對禁止此種與兒童相關之運用。然而，依據該前言，WP29建議，作為原則，控管者不應援引第22條第2款中之例外以證明運用之正當性。

There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare. If so, the processing may be carried out on the basis of the exceptions in Article 22(2)(a), (b) or (c) as appropriate.

然而，在某些情況下，控管者有必要執行對兒童有法律或類似重大影響之純自動化決策（包含剖析），例如為保護兒童之福祉。若如此，則可依據第22條第2項第a款、第b款或第c款中之例外情形酌情執行運用。

In those cases there must be suitable safeguards in place, as required by Article 22(2)(b) and 22(3), and they must therefore be appropriate for children. The controller must ensure that these safeguards are effective in protecting the rights, freedoms and legitimate interests of the children whose data they are processing.

在這些情況下，須依照第22條第2項第b款和第22條第3項之要求採取適合於兒童之適當安全維護措施。控管者必須確保這些安全維護措施能夠有效地保護資料正被運用的兒童之權利、自由和正當利益。

The need for particular protection for children is reflected in recital 38, which says:

對兒童之特殊保護需求反映於前言第38點中，該前言指出：

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes *of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.*
>
> 有鑑於兒童可能未盡知悉其個人資料運用之風險、後果及相關安全維護措施與其權利，兒童就其個人資料應受到特別保護。此種具體保護應適用於兒童個人資料之使用，特別是當該運用之目的係*為行銷、建立個性或用戶剖析檔案，以及當服務直接提供予兒童時蒐集與其相關之個人資料。*

[44] Recital 71 – "such measure should not concern a child".
前言第71點 – 「此類措施不應涉及兒童」。

Article 22 does not prevent controllers from making solely automated decisions about children, if the decision will not have a legal or similarly significant effect on the child. However, solely automated decision making which influences a child's choices and behaviour could potentially have a legal or similarly significant effect on them, depending upon the nature of the choices and behaviours in question.

若決策不會對兒童產生法律或類似重大之影響，第22條並不禁止控管者作出與兒童相關之純自動化決策。然而，影響兒童選擇和行為之純自動化決策是否可能會對其產生法律或類似之重大影響，需具體取決於系爭選擇和行為之性質。

Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.[45] Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences.[46]

由於兒童代表了一種較弱勢的社會群體，因此組織通常不應基於行銷目的對其進行剖析。[45]兒童在網絡環境中特別容易受到影響，且更容易受到行為廣告之影響。例如，在網路遊戲中，剖析可用來鎖定演算法所認為更有可能在遊戲上花錢之玩家以及提供更個人化之廣告。兒童的年齡和成熟程度可能會影響其理解此種行銷背後動機或後果之能力。[46]

Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children; it may also be possible to develop existing codes.[47]

第40條第2項第g款明確提及制定包含兒童安全維護措施之行為守則；亦可改善現有之守則。[47]

---

[45] The WP29 Opinion 02/2013 on apps on smart devices (WP202), adopted on 27 February 2013, under the specific section 3.10 on Children, specifies at page 26 that "data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, since this will be outside of the scope of the child's understanding and therefore exceed the boundaries of lawful processing".
WP29第02/2013號意見關於智能設備應用程式（WP202），於2013年2月27日通過，關於兒童之具體章節3.10，於第26頁指出「資料控管者不應直接或間接為行為廣告之目的而運用兒童資料，因該運用將不在兒童理解範圍之內，因而超出了合法運用之範圍。」

[46] An EU study on the impact of marketing through social media, online games and mobile applications on children's behaviour found that marketing practices have clear impacts on children's behaviour. This study was based on children aged between 6 and 12 years.
歐盟一項關於透過社群媒體、網路遊戲和手機應用程式對兒童行為影響之研究發現，行銷活動對兒童之行為有明顯的影響。此項研究係針對6至12歲之間的兒童。

[47] One example of a code of conduct dealing with marketing to children is that produced by FEDMA Code of conduct, explanatory memorandum, available at: http://www.oecd.org/sti/ieconomy/2091875.pdf Accessed 15 May 2017. See, in particular: "6.2 Marketers targeting children, or for whom children are likely to constitute a section of their audience, should not exploit children's credulity, loyalty, vulnerability or lack of experience.;

VI. Data protection impact assessments (DPIA) and Data Protection Officer (DPO)
個資保護影響評估（DPIA）和個資保護長（DPO）

Accountability is an important area and an explicit requirement under the GDPR. [48]
課責性是GDPR的一個重要領域且有明確之要求。[48]

As a key accountability tool, a DPIA enables the controller to assess the risks involved in automated decision-making, including profiling. It is a way of showing that suitable measures have been put in place to address those risks and demonstrate compliance with the GDPR.
作為課責性之關鍵工具，DPIA使控管者能夠評估自動化決策（包含剖析）中涉及之風險。DPIA是一種顯示已採取適當措施以因應這些風險並證明已遵守GDPR之方式。

Article 35(3) (a) highlights the need for the controller to carry out a DPIA in the case of:
第35條第3項第a款強調控管者在下列情況執行DPIA之必要性：

> *a systematic and extensive evaluation* of personal aspects relating to natural persons which is *based on* automated processing, *including* profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> *基於*自動化運用（*包含*剖析）對與自然人相關之個人面向進行*系統性*和*廣泛性*的評估，且基於該評估所作成之決策將對自然人產生法律效果或類似重大影響；

Article 35(3)(a) refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3) (a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is *not* wholly automated, as well as solely automated decision-making defined in Article 22(1).
第35條第3項第a款提及之評估包括「基於」自動化運用之剖析和決策，而非「純」自動化運用。我們認為此意味著第35條第3項第a款將適用於有法律或類似重大影響之*非*完全自動

6.8.5 Marketers should not make a child's access to a website contingent on the collection of detailed personal information. In, particular, special incentives such as prize offers and games should not be used to entice children to divulge detailed personal information."
針對兒童行銷行為守則之示例可參考FEDMA行為守則所發行之解釋性備忘錄，請參閱：http：//www.oecd.org/sti/ieconomy/2091875.pdf 瀏覽日期：2017年5月15日。特別參閱：「6.2 針對兒童之行銷人員，或兒童可能構成其部分觀眾之行銷人員，不應利用兒童的易輕信、忠誠、弱勢及缺乏經驗；6.8.5 行銷人員不應將蒐集詳細個人資料作為兒童瀏覽網站之條件。尤其是，不得使用獎品和遊戲等特殊獎勵措施誘使兒童揭露詳細之個人資訊。」

[48] As required by the GDPR Article 5(2).
依據GDPR第5條第2項之要求。

化決策（包含剖析），以及第22條第1項定義之純自動化決策。

If the controller envisages a 'model' where it takes *solely* automated decisions having a *high impact* on individuals based on *profiles* made about them and it *cannot* rely on the individual's consent, on a contract with the individual or on a law authorising this, the controller should not proceed.

若控管者預設一種「模型」，*而該模型係基於與個人相關之剖析檔案而做出對其產生高度影響之純自動*化決策，*當運用無法依賴個人之同意、與個人之契約或法律授權時，則控管者不應繼續該行為。*

The controller can still envisage a 'model' of decision-making based on profiling, by significantly increasing the level of human intervention so that the model is *no longer a fully automated decision making process*, although the processing could still present risks to individuals' fundamental rights and freedoms. If so the controller must ensure that they can address these risks and meet the requirements described in Chapter III of these Guidelines.

控管者仍可預設基於剖析之決策「模型」，*透過顯著提高人為參與程度，使該模型不再屬於一種完全自動化的決策程序*,即使此運用仍可能對當事人的基本權利和自由帶來風險 。*如是，控管者必須確保其有能力因應這些風險並滿足本指引第*III*章中所描述之要求。*

A DPIA can also be a useful way for the controller to identify what measures they will introduce to address the data protection risks involved with the processing. Such measures[49] could include:

DPIA*亦可用於協助控管者識別將採行何種措施以因應運用所涉及之資料保護風險，這些措施*[49]*可包括：*

- informing the data subject about the existence of and the logic involved in the automated decision-making process;
  告知當事人自動化決策程序之存在以及所涉之邏輯；
- explaining the significance and envisaged consequences of the processing for the data subject;
  解釋運用對當事人之重要性和預設之後果；
- providing the data subject with the means to oppose the decision; and
  為當事人提供對決策異議之方式；及
- allowing the data subject to express their point of view.
  允許當事人表達其觀點。

[49] Mirroring the requirements in Article 13(2)(f), Article 14(2)(g) and Article 22(3).
*比照第*13*條第*2*項第*f*款、第*14*條第*2*項第*g*款、和第*22*條第*3*項之要求。*

Other profiling activities may warrant a DPIA, depending upon the specifics of the case. Controllers may wish to consult the WP29 guidelines on DPIAs[50] for further information and to help determine the need to carry out a DPIA.

其他可能需要DPIA之剖析活動將取決於案件之具體情況。控管者可查閱WP29關於DPIA之指引[50]，以獲取更多資訊，並協助確認執行DPIA之必要性。

An additional accountability requirement is the designation of a DPO, where the profiling and/or the automated decision-making is a core activity of the controller and requires regular and systematic monitoring of data subjects on a large scale (Article 37(1)(b).[51]

此外，當剖析和/或自動化決策係控管者之核心業務，且需經常性和系統性地大規模監控當事人時（第37條第1項第b款），額外之課責性要求為指定DPO [51]

[50] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 4 April 2017.. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.
29條資料保護工作小組。第2016/679號規則關於個資保護影響評估（DPIA）指引以及確認運用是否「可能造成高風險」。2017年4月4日.. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。瀏覽日期：2017年4月24日。

[51] Article 29 Data Protection Working Party. Guidelines on Data Protection Officer (DPOs). 5 April 2017; http://ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=612048 Accessed 22 January 2018.
29條資料保護工作小組。個資保護長（DPOs）指引。2017年4月5日;
http://ec.europa.eu/newsroom/article29/item-detail.cfm？item_id = 612048。瀏覽日期：2018年1月22日。

ANNEX 1 - Good practice recommendations
附錄1－ 優良實務做法建議

The following good practice recommendations will assist data controllers in meeting the requirements of the GDPR provisions on profiling and automated decision making.[52]
以下優良實務作法建議將有助於資料控管者符合GDPR關於剖析和自動化決策之規定。[52]

Article 條文	Issue 爭點	Recommendation 建議
5(1)(a),12, 13, 14 第5條第1項第a款、第12條、第13條、第14條	Right to have Information 取得資訊之權利	Controllers should consult the WP29 Guidelines on transparency WP260 for general transparency requirements. 控管者應參考WP29透明化之指引（WP260）關於一般透明化之要求。 In addition to the general requirements, when the controller is processing data as defined in Article 22, they must provide meaningful information about the logic involved. 除一般要求外，當控管者運用第22條定義之資料時，必須提供有關所涉邏輯之有意義資訊。 Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject, for example: 控管者不需提供有關演算法或機器學習如何作業之複雜數學解釋，而應考量使用清晰且全面性之方式將資訊傳達予當事人，例如： ● the categories of data that have been or will be used in the profiling or decision-making process; 已經或將要於剖析或決策程序中使用之資料類型； ● why these categories are considered pertinent; 為何這些類型被認為係相關的；

[52] Controllers also need to ensure they have robust procedures in place to ensure that they can meet their obligations under Articles 15 – 22 in the timescales provided for by the GDPR.
控管者亦需確保其擁有可靠之程序，以確保能夠在GDPR規定之時間範圍內符合第15-22條規定之義務。

		• how any profile used in the automated decision-making process is built, including any statistics used in the analysis; 如何建構自動化決策程序中所使用之任何剖析檔案，包括分析中使用之任何統計資訊； • why this profile is relevant to the automated decision-making process; and 為何此類剖析檔案與自動化決策程序相關；及 • how it is used for a decision concerning the data subject. 如何將其使用於與當事人相關之決策。 Such information will generally be more relevant to the data subject and contribute to the transparency of the processing. 這些資訊通常與當事人更相關，並有助於運用之透明化。 Controllers may wish to consider visualisation and interactive techniques to aid algorithmic transparency[53]. 控管者可能希望考量視覺化和互動式技術以協助演算法之透明化[53]。
6(1)(a) 第6條第1項第a款	Consent as a Basis for processing 以同意作為運用之基礎	If controllers are relying upon consent as a basis for processing they should consult the WP29 Guidelines on consent WP259. 若控管者以同意作為其運用之基礎時，則應參考WP29關於同意之指引（WP259）。
15 第15條	Right of Access 近用權	Controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it. 控管者可能希望考量實施某種機制使當事人可查閱其剖析檔案，包括建立該剖析檔案之詳細資訊及資料來源。

[53] Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017. Page 87, paragraph 194, March 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Accessed 24 April 2017
英國資訊委員辦公室 – 大數據、人工智慧、機器學習和資料保護 2.0 版本，03/2017。第 87 頁，第 194 段， 2017 年 3 月. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf 瀏覽日期：2017 年 4 月 24 日。

16 第16條	Right to rectification 更正權	Controllers providing data subjects with access to their profile in connection with their Article 15 rights should allow them the opportunity to update or amend any inaccuracies in the data or profile. This can also help them meet their Article 5(1) (d) obligations. 控管者為當事人提供與其第15條權利相關之剖析檔案近用權，應可使當事人有機會更新或修改資料或剖析檔案中之任何不正確之處。此亦有助於控管者符合第5條第1項第d款之義務。 Controllers could consider introducing online preference management tools such as a privacy dashboard. This gives data subjects the option of managing what is happening to their information across a number of different services – allowing them to alter settings, update their personal details, and review or edit their profile to correct any inaccuracies. 控管者可優先考量使用網路管理工具，例如隱私儀表板。如此可提供當事人管理跨多項不同服務之資訊之選擇 – 允許其更改設置、更新個人詳細資訊、及查看或編輯個人剖析檔案以更正任何不正確之處。
21(1) and (2) 第21條第1項和第2項	Right to object 拒絕權	The right to object in Article 21(1) and (2) has to be explicitly brought to the attention of the data subject and presented clearly and separately from other information (Article 21(4). 必須明確使當事人注意到第21條第1項和第2項之拒絕權，並以清楚並與其他資訊區別之方式呈現（第21條第4項）。 Controllers need to ensure that this right is prominently displayed on their website or in any relevant documentation and not hidden away within any other terms and conditions. 控管者需確保在其網站或任何相關文件中突顯此項權利，且不得隱藏於任何其他條款和條件中。
22 and Recital 71 第22條及	Appropriate safeguards 適當安全維	The following list, though not exhaustive, provides some good practice suggestions for controllers to consider when making solely automated decisions, including profiling (defined in

前言第71點	護措施	Article 22(1)): 以下列表雖非詳盡無遺，但對控管者提供了一些優良實務作法之建議，使其在執行純自動化決策（包含剖析）時得加以考量（定義於第22條第1項）： ● regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise; 定期對其系統進行品質保證檢查，以確保個人獲得公正待遇且不受到歧視，無論係基於特種類型之個人資料抑或其他資料； ● algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results; 演算法之稽核 – 測試機器學習系統所使用和研發之演算法，以證明其確實依預設執行，且不產生歧視性、錯誤或不合理之結果； ● for independent 'third party' auditing (where decision-making based on profiling has a high impact on individuals), provide the auditor with all necessary information about how the algorithm or machine learning system works; 對於獨立「第三方」之稽核（當基於剖析之決策對個人有重大影響時），向稽核員提供有關演算法或機器學習系統運作方式之所有必要資訊； ● obtaining contractual assurances for third party algorithms that auditing and testing has been carried out and the algorithm is compliant with agreed standards; 取得第三方演算法之契約保證，確認稽核和測試已被執行，以及演算法符合議定之標準； ● specific measures for data minimisation to incorporate clear

		retention periods for profiles and for any personal data used when creating or applying the profiles; 資料最小化之具體措施，以體現剖析檔案及用於建立或應用剖析檔案時所使用任何個人資料之明確的留存期限； ● using anonymisation or pseudonymisation techniques in the context of profiling; 在剖析背景下使用匿名化或假名化技術； ● ways to allow the data subject to express his or her point of view and contest the decision; and, 允許當事人表達其觀點並對決策提出異議之方式；以及 ● a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries. 在特定情況下執行人為參與之機制，例如在傳遞自動化決策予當事人時，提供申訴程序之連結、議定之審閱期間及詢問之指定聯絡方式。 Controllers can also explore options such as: 控管者亦可採取以下選項： ● certification mechanisms for processing operations; 運用作業之認證機制； ● codes of conduct for auditing processes involving machine learning; 涉及機器學習之稽核程序行為守則； ● ethical review boards to assess the potential harms and benefits to society of particular applications for profiling. 道德審查委員會，以評估特定剖析應用對社會之潛在危害和益處。

ANNEX 2 – Key GDPR provisions
附錄2 – GDPR主要條款

Key GDPR provisions that reference general profiling and automated decision-making
GDPR 中關於一般剖析和自動化決策之主要條款

Article 條文	**Recital** 前言	**Comments** 評論
3(2)(b) 第3條 第2項 第b款	**24** 第24點	The monitoring of data subjects' behaviour as far as their behaviour takes place within the Union. 監控當事人行為，只要其行為發生於歐盟境內。 **Recital 24** **前言第24點** "….tracked on the internet ……use of personal data processing techniques which consist of profiling a natural person, *particularly in order to take decisions* concerning her or him or for analysing or predicting her or his personal preferences, behaviours or attitudes". 「.....在網路上追蹤..... 包含以個人資料運用技術對自然人進行剖析的潛在後續利用，*尤其是為了作成*與其有關的*決策*，或為分析或預測其個人偏好、行為及態度」。
4(4) 第4條 第4項	**30** 第30點	**Article 4(4)** definition of profiling 第4條第4項剖析之定義 **Recital 30** **前言第30點** "online identifiers …., such as Internet Protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags… may leave traces which, in particular when combined with unique identifiers and other information received by the servers, *may be used to create profiles of the natural persons and identify them*." 「網路識別碼.....，例如網際網路協定位址，瀏覽歷程識別碼或其他識別工具例如無線射頻識別標籤...，可能留下足跡，尤其是當與伺服器所接

		收之獨特識別碼及其他資訊相結合時，*可能用於建立與自然人相關之剖析檔案並對其加以識別*。」
5 and 6 第5條及第6條	**72** 第72點	**Recital 72:** **前言第72點：** "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing **(Article 6)** or data protection principles **(Article 5)**." 「剖析受本法規治理個人資料運用之規則約束，例如運用之法律依據（**第6條**）或資料保護原則（**第5條**）。」
8 第8條	**38** 第38點	Use of children's personal data for profiling. 使用兒童個人資料進行剖析。 **Recital 38:** **前言第38點：** "Children merit specific protection ….. in particular,…to the use of personal data of children for the purposes of….creating personality or user profiles." 「兒童應受特別保護.....尤其是.....為了....建立個性或用戶之剖析檔案，而使用兒童之個人資料。」
13 and 14 第13條及第14條	**60** 第60點	Right to be informed. 被告知權。 **Recital 60:** **前言第60點：** "Furthermore, the data subject shall *be informed of the existence of profiling and the consequences of such profiling* ." 「此外，應*告知當事人剖析之存在以及此類剖析之後果*。」
15 第15條	**63** 第63點	Right of access. 近用權 **Recital 63:** **前言第63點：** "right to know and obtain communication…..with regard to the purposes for

		which the personal data are processed,…..and, *at least* when based on profiling, the consequences of such profiling". 「知情及獲得溝通之權利.....就個人資料運用目的而言，.....且，至少在基於剖析之情況下，此類剖析之後果」。
21(1)(2) and (3) 第21條 第1項 第2項 及 第3項	**70** 第70點	Right to object to profiling. 拒絕剖析之權利 **Recital 70** **前言第70點** "…the right to object to such processing, including profiling to the extent that it is related to such direct marketing." 「…拒絕此類運用之權利，包括與此類行銷相關之剖析。」
23 第23條	**73** 第73點	**Recital 73:** **前言第73點：** "Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…" to safeguard specific objectives of general public interest. 「關於具體原則之限制和關於.....拒絕權及基於剖析所為決策之限制.....可依據歐盟或成員國法律加以施行，當於民主社會中所必須且符合比例原則時...」為維護一般公眾利益之特定目的。
35(3)(a) 第35條 第3項 第a款	**91** 第91點	A DPIA is required in the case of "a systematic and extensive evaluation of personal aspects relating to natural persons which is *based* on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;" **Covers decision-making including profiling that is not solely automated.** 在「*基於*自動化運用（包含剖析）對與自然人相關之個人面向進行系統性和廣泛之評估，且基於該評估所為之決策造成與自然人相關之法律效果或對該自然人造成類似重大之影響時」，需執行DPIA。**此規定涵蓋包含剖析之非純自動化決策**。

Key GDPR provisions that reference automated decision-making as defined in Article 22
GDPR 中關於第 22 條定義下自動化決策之主要條款

Article 條文	**Recital** 前言	**Comments** 評論
13(2)(f) And **14(2)(g)** 第13條 第2項 第f款 及 第14條 第2項 第g款	**61** 第61點	Right to be informed about: 就以下資訊有被告知之權利：· ● the existence of automated decision-making under **A22(1)** and **(4);** 依據第22條第1項和第4項自動化決策之存在； ● meaningful information about the logic involved; 所涉邏輯之有意義資訊； ● significance and envisaged consequences of such processing. 此類運用之重要性和預設之後果。
15(h) 第15條 第h款		Specific access rights to information about the existence of solely automated decision-making, including profiling. 對純自動化決策（包含剖析）資訊之具體近用權。
22(1) 第22條 第1項	**71** 第71點	Prohibition on decision-making based solely on automated processing, including profiling, which produces legal/similarly significant effects. 禁止會產生法律/或類似重大影響之純自動化運用之決策（包含剖析）。 In addition to the explanation provided in the main body of the guidelines, the following points expand on the rationale for reading Article 22 as a prohibition: 除了本指引主文中提供之解釋外，下列幾點擴大了將第22條作為禁止解釋之理由： ● Although Chapter III is about the rights of the data subject, the provisions in Articles 12 - 22 are not exclusively concerned with the *active* exercise of rights. Some of the rights are *passive*; they do not all

		relate to situations where the data subject takes an action i.e. makes a request or a complaint or a demand of some sort. Articles 15-18 and Articles 20-21 are about the data subject actively exercising their rights, but Articles 13 &14 concern duties which the data controller has to fulfil, without any active involvement from the data subject. So the inclusion of Article 22 in that chapter does not in itself mean that it is a right to object; 雖然第III章涉及當事人之權利，但第12-22條之規定並非僅涉及*積極*行使權利。某些權利係*被動的*；這些權利並非皆與當事人採取行動之情況相關，即提出要求或申訴或某種請求。第15-18條和第20-21條係有關當事人積極行使其權利之情況，然第13和14條涉及資料控管者必須履行之義務，而不需當事人任何積極之參與。因此，於該章節中列入第22條並不意味著此係屬於拒絕權； ● Article 12(2) talks about the exercise of 'data subject rights under Articles 15 to 22; but this does not mean that Article 22(1) itself has to be interpreted as a right. There *is* an active right in A22, but it is part of the safeguards which have to be applied in those cases where automated decision making is allowed (Articles 22(2)(a-c)) - the right to obtain human intervention, express his or her point of view and to contest the decision. It only applies in those cases, because carrying out the processing described in Article 22(1) on other bases is prohibited; 第12條第2項論及依據第15條至第22條行使「當事人之權利」； 然此並不意味著第22條第1項本身必須被解釋為一項權利。第22條中*有*一種積極之權利，然此適用於在允許自動化決策之情況下作為安全維護措施之一部分（第22條第2項第a-c款）－ 即獲得人為參與、表達觀點和質疑決策之權利。該條款僅適用於這些情況，因在其他基礎上進行第22條第1項所述之運用皆是被禁止的； ● Article 22 is found in a section of the GDPR called "Right to object **and** automated individual decision-making", implying that Article 22 is *not* a right to object like Article 21. This is further emphasised by the lack in Article 22 of an equivalently explicit information duty as that found in Article 21(4); 第22條列於於GDPR關於「拒絕權**及**自動化個人決策」之章節中，

		此意味著第22條*並非*屬於第21條下之拒絕權。第22條缺乏與第21條第4項同等明確之資訊義務亦進一步強化此一觀點； ● If Article 22 were to be interpreted as a right to object, the exception in Article 22(2)(c) would not make much sense. The exception states that automated decision-making can still take place if the data subject has given explicit consent (see below). This would be contradictory as a data subject cannot object and consent to the same processing; 若第22條被解釋為是一種拒絕權，第22條第2項第c款中之例外情形便失去意義。該條之但書規定，若當事人已明確表示同意，則仍可進行自動化決策（請參閱下文）。如此是自相矛盾的，因當事人就同一個運用不得同時拒絕並同意； ● An objection would mean that human intervention must take place. Article 22(2)(a) and (c) exceptions override the main rule in Article 22(1), but only as long as human intervention is available to the data subject, as specified in Article 22(3). Since the data subject (by objecting) has already requested human intervention, Article 22(2)(a) and (c) would automatically be circumvented in every case, thus rendering them meaningless in effect. 拒絕意味著必須進行人為參與。第22條第2項第a款及第c款規定之例外優先於第22條第1項之主要規定，但只有在依據第22條第3項之規定，當人為參與適用於當事人之情況下才成立。由於當事人（透過拒絕）已要求人為參與，第22條第2項第a款和第c款將在所有情況下自動被規避，從而使其毫無意義。 **Recital 71:** **前言第71點：** "…Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" …… "*Such measure should not concern a child*" 「...此類運用包含「剖析」，而其係由任何形式之自動化運用個人資料所

		組成，以評估與自然人相關之個人面向，尤其是分析或預測關於當事人於工作中之表現、經濟狀況、健康、個人偏好或興趣、可靠性或行為、所在位置或移動」.....「*此類措施不應涉及兒童*」
22(2)(a-c) **第22條第(2)項第a-c款**	**71** **第71點**	**Article 22(2)** lifts the prohibition for processing based on **(a)** the performance of or entering into a contract, **(b)** Union or Member state law, or **(c)** explicit consent. **第22條第2項**基於（**a**）履行或簽訂契約、（**b**）歐盟或成員國法律、或（**c**）明確之同意，可免除對運用之禁止。 **Recital 71** provides further context on **22(2)(b)** and says that processing described in **A22(1):** **前言第71點**提供了關於**第22條第2項第b款**之進一步內容，並指出**第22條第1項**中描述之運用： "should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller…" 「在控管者所適用之歐盟或成員國法律明確授權之情況下，包括依據歐盟機構或國家監管機構之規則、標準和建議而對詐欺和逃稅進行監測和為預防之目的，以及確保控管者所提供服務之安全性和可靠性...」
22(3) **第22項第3款**	**71** **第71點**	**Article 22 (3) and Recital 71** also specify that even in the cases referred to in **22(2)(a)** and **(c)** the processing should be subject to suitable safeguards. 第22條第3項和前言第71點亦規定，即使在第22條第2項第a款和第c款所述之情況下，運用仍應受到適當安全維護措施之保障。 **Recital 71:** **前言第71點:** "which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge

		the decision. Such measure should not concern a child." 「其中應包含當事人之具體資訊以及獲得人為參與、表達觀點、獲得評估後所作決策之理由、及質疑該決策之權利。此種措施不應涉及兒童。」
23 **第23條**	**73** **第73點**	**Recital 73:** **前言第73點:** "Restrictions concerning specific principles and concerning …….the right to object and decisions based on profiling …….may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society…" to safeguard specific objectives of general public interest. 「關於具體原則之限制和關於.....拒絕權及基於剖析所為決策之限制.....可依據歐盟或成員國法律加以施行,當於民主社會中所必須及符合比例原則時..」為維護一般公共利益之特定目的。
35(3)(a) **第35條** **第3項** **第a款**	**91** **第91點**	Requirement to carry out a DPIA. 執行DPIA之要求。
47(2)(e) **第47條** **第2項** **第e款**		Binding corporate rules referred to in **47(1)** should specify at least "…….the right not to be subject to decisions based solely on automated processing, including profiling in accordance with **Article 22**..." 第47條第1項所述具有約束力之企業守則應至少表明「.....不受純自動化運用所做決策拘束之權利，包含依據第22條執行之剖析...」

ANNEX 3 - Further reading

附錄3 - 延伸閱讀

These Guidelines take account of the following:

本指引參考以下文件：

- WP29 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted 13 May 2013;
- WP29 Opinion 2/2010 on online behavioural advertising, WP171;
- WP29 Opinion 03/2013 on Purpose limitation, WP 203;
- WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217
- WP29 Statement on the role of a risk-based approach to data protection legal frameworks, WP218;
- WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223;
- WP29 Guidelines on Data Protection Officers (DPOs), WP243;
- WP29 Guidelines on identifying a controller or processor's lead supervisory authorityWP244;
- WP29 Guidelines on consent,WP259
- WP29 Guidelines on transparency, WP260
- Council of Europe. Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling;
- Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 01/2017
- Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017
- Office of the Australian Commissioner - Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016
- European Data Protection Supervisor (EDPS) Opinion 7/2015 – Meeting the challenges of big data, 19 November 2015
- Datatilsynet – Big Data – privacy principles under pressure 09/2013
- Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data - Draft explanatory report on the modernised version of CoE Convention 108, August 2016
- Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy. Report, November 2015

- European Data Protection Supervisor – Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit
- Joint Committee of the European Supervisory Authorities. Joint Committee Discussion Paper on the use of Big Data by financial institutions 2016-86. https://www.esma.europa.eu/sites/default/files/library/jc-2016 86_discussion_paper_big_data.pdf.
- Commission de la protection de la vie privée. Big Data Rapport https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20vo or%20MindMap%2022-02-17%20fr.pdf.
- United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. Research paper, posted 24 May 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com. Showing the Algorithms behind New York City Services. https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city- services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Accessed 24 August 2017
- Council of Europe. Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children's rights in the digital environment (revised draft, 25 July 2017). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren . Accessed 31 August 2017
- Unicef. Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accessed 31 August 2017
- House of Lords. Growing up with the internet. Select Committee on Communications, 2nd Report of Sessions 2016 – 17.

https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Accessed 31 August 2017

- Sandra Wachter, Brent Mittelstadt and Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, 28 December 2016. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/ . Accessed 13 December 2017
- Sandra Wachter, Brent Mittelstadt and Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR, 6 October 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Accessed 13 December 2017
- Australian Government. Better Practice Guide, Automated Assistance in Administrative Decision- Making. Six steps methodology, plus summary of checklist points Part 7 February 2007. https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf. Accessed 9 January 2018

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN

WP 242 rev.01

Guidelines on the right to data portability
關於資料可攜權之指引

Adopted on 13 December 2016

2016 年 12 月 13 日通過

As last Revised and adopted on 5 April 2017

2017 年 4 月 5 日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

TABLE OF CONTENTS 目錄

Executive summary

摘要

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access but differs from it in many ways. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.

GDPR第20條創造了一種新的資料可攜權，此權利與近用權密切相關，卻又在許多面向與之不同。可攜權允許當事人得以結構性、一般性和機器可讀性之格式接收其提供予控管者之個人資料，並將這些資料傳輸至另一資料控管者。此項新權利之目的係賦予當事人權利，並使其能更有效控制與自身相關之個人資料。

Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.

由於資料可攜權允許將個人資料從一資料控管者直接傳輸至另一資料控管者，因此該權利亦是支持歐盟個人資料之自由流通和促進控管者競爭的重要工具。資料可攜權將增進不同服務提供商之間的轉換，從而促進在數位單一市場背景下開發新服務。

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing* (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies. In this regard, WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form.

本意見為GDPR中資料可攜權之解釋和執行方式提供了指導。其目的在於討論資料可攜權及其範圍。本意見闡明了此一新權利之適用條件，同時考量到資料運用的法律依據（當事人同意或為履行契約所必要）以及此權利僅適用於由當事人提供之個人資料的事實。本意見亦提供了具體之示例和標準來解釋該權利之適用情形。於此面向上，

29條工作小組認為資料可攜權涵蓋當事人有意識和積極提供之資料以及因當事人之行為而產生之個人資料。此項新權利不得被損害，且不限於當事人直接傳達之個人資訊，例如，線上表格。

As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.
作為一種優良實務範例，資料控管者應開始建立有助於回應資料攜帶請求之方法，例如可供下載之工具和應用程式介面。控管者應確保個人資料以結構性、一般性和機器可讀性之格式傳輸，並應鼓勵其在執行資料攜帶請求時，須確保所提供資料格式之互通性。

The opinion also helps data controllers to clearly understand their respective obligations and recommends best practices and tools that support compliance with the right to data portability. Finally, the opinion recommends that industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.
本意見亦有助於資料控管者清楚地瞭解各自之義務，並就支持遵守資料可攜權的優良實務範例和工具提供建議。最後，本意見建議產業相關者和同業公會在一套通用且可互通之標準和格式上協同作業，以實現資料可攜權之需求。

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

I. Introduction
導言

Article 20 of the General Data Protection Regulation (GDPR) introduces a new right of data portability. This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. This right, which applies subject to certain conditions, supports user choice, user control and user empowerment.
一般資料保護規則（GDPR）第20條導入了新的資料可攜權。該權利允許當事人得以結構性、一般性和機器可讀性之格式接收其提供予控管者之個人資料，並不受妨礙地將這些資料傳輸至另一資料控管者。在符合特定要件下，此權利支持用戶選擇、用戶控制和用戶授權。

Individuals making use of their right of access under the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller when providing the requested information. **The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another** (whether to their own systems, the systems of trusted third parties or those of new data controllers).
過去個人依據第95/46/EC號資料保護指令行使近用權時，會受限於資料控管者在提供所請求資訊時所選擇之格式。**新的資料可攜權旨在賦予當事人關於自身個人資料之能力，該權利有助於當事人輕易地將個人資料從一個IT環境中移動、複製或傳輸至另一個IT環境**（無論是其本身之系統、可信任第三方之系統亦或其他新的資料控管者之系統）。

By affirming individuals' personal rights and control over the personal data concerning them, data portability also represents an opportunity to "re-balance" the relationship between data subjects and data controllers[1].
透過確認當事人之個人權利和相關個人資料之控制，資料可攜性亦代表了一種機會，可「再平衡」當事人和資料控管者之間的關係[1]。

Whilst the right to personal data portability may also enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition. In particular, article 20 does not limit portable data to those which are necessary or useful for switching services[2].
雖然個人資料可攜權得增加服務間之競爭（透過促進服務轉換），但GDPR所規範的是個人資料而非競爭。尤其是，第20條並未將可攜資料限縮於為轉換服務所必需或有用之資料

[1] The primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem.
資料可攜性之主要目的係增強當事人對其個人資料之控制，並確保其在資料生態系統中扮演積極之角色。

[2] 。

Although data portability is a new right, other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services[3]). Some synergies and even benefits to individuals may emerge between the different types of portability if they are provided in a combined approach, even though analogies should be treated cautiously.
雖然資料可攜權係一項新的權利，但其他類型之可攜性其實已存在或正在其他法律領域中進行討論（例如，在終止契約、通訊漫遊服務和跨境存取服務之背景下[3]）。在不同類型可攜性間，若以結合之方式提供可攜性，可能會出現對當事人的一些增效作用甚至益處，然類推適用時仍應謹慎。

This Opinion provides guidance to data controllers so that they can update their practices, processes and policies, and clarifies the meaning of data portability in order to enable data subjects to efficiently use their new right.
本意見為資料控管者提供指導，使控管者可更新其實務做法、程序和政策，並闡明資料可攜性之含義，使當事人得有效地行使此一新權利。

II. What are the main elements of data portability?
資料可攜性之主要要件為何？

The GDPR defines the right of data portability in Article 20 (1) as follows:
GDPR第20條第1項對資料可攜權之定義如下：

> *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided [...]*
> *當事人應有權利以結構性、一般性和機器可讀性之格式接收其提供予控管者與自身相關之個人資料，並有權利不受其提供個人資料之控管者妨礙，將這些資料傳輸至另一資料控管者[...]*

- **A right to receive personal data**

[2] For example, this right may allow banks to provide additional services, under the user's control, using personal data initially collected as part of an energy supply service.
例如，該權利可在用戶的控制下，允許銀行使用當初因為能源供應服務而蒐集之個人資料以提供附加服務。
[3] See European Commission agenda for a digital single market: https://ec.europa.eu/digital-agenda/en/digital-single-market, in particular, the first policy pillar "Better online access to digital goods and services".
請參閱歐盟執委會關於數位單一市場之議程：https://ec.europa.eu/digital-agenda/en/digital-single-market，尤其是第一項政策支柱「更優質之網路數位商品和服務之存取」。

接收個人資料之權利

Firstly, data portability is a **right of the data subject to receive a subset of the personal data** processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.

首先，資料可攜性是一種**當事人接收**由資料控管者運用之相關**個人資料子集**，並為進一步個人使用而儲存這些資料**的權利**。此種儲存可在私人設備或私人雲端上，不一定需將資料傳輸至另一資料控管者。

In this regard, data portability complements the right of access. One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves. These data should be received "*in a structured, commonly used and machine-readable format"*. For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint[4].

在此情形下，資料可攜性補充了近用權。資料可攜性的一個特點即在於為當事人提供了一種簡單的方式來管理和再使用個人資料。這些資料必須*以「結構性、一般性和機器可讀性之格式」接收*。例如，當事人可能有興趣從串流音樂服務中取得當前的播放列表（或收聽曲目的歷史紀錄），以找出特定曲目收聽次數，或用以比對在另一平台上想要購買或收聽的音樂。同樣的，當事人亦可能想從其網路郵件應用程式中取得聯絡人清單，例如為建立婚禮清單，抑或取得有關使用不同會員卡的購買資訊，或評估其碳足跡[4]。

- **A right to transmit personal data from one data controller to another data controller**

  將個人資料從一資料控管者傳輸至另一資料控管者之權利

Secondly, Article 20(1) provides data subjects with the **right to transmit personal data from one data controller to another data controller** "without hindrance". Data can also be transmitted directly from one data controller to another on request of the data subject and where

[4] In these cases, the processing performed on the data by the data subject can either fall within the scope of household activities, when all the processing is performed under the sole control of the data subject, or it can be handled by another party, on the data subject's behalf. In the latter case, the other party should be considered as data controller, even for the sole purpose of personal data storage, and must comply with the principles and obligations laid down in the GDPR.

在這些情形下，當所有運用皆係在當事人的單獨控制下所進行，由當事人對資料進行之運用可能落入家庭活動範圍，抑或在代表當事人之情況下，由另一方為之。若為後者之情形，該另一方應被視為資料控管者，即使僅用於個人資料之儲存，亦須遵守GDPR中規定之原則和義務。

it is technically feasible (Article 20(2)). In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability[5] but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible[6]. The GDPR does, however, prohibit controllers from establishing barriers to the transmission.

其次，第20條第1項規定當事人**有權利**「不受妨礙地」**將個人資料從一資料控管者傳輸至另一資料控管者**。在技術可行之情況下，依據當事人之請求，資料亦可直接從一資料控管者直接傳輸至另一資料控管者（第20條第2項）。於此面向，前言第68點鼓勵資料控管者建立互通之格式，以實現資料可攜性[5]，但不至課予控管者義務，要求採用或維護技術上相容之運用系統[6]。然而，GDPR確實禁止控管者設置傳輸障礙。

In essence, this element of data portability provides the ability for data subjects not just to obtain and reuse, but also to transmit the data they have provided to another service provider (either within the same business sector or in a different one). In addition to providing consumer empowerment by preventing "lock-in", the right to data portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject's control[7]. Data portability can promote the controlled and limited sharing by users of personal data between organisations and thus enrich services and customer experiences[8]. Data portability may facilitate transmission and reuse of personal data concerning users among the various services they are interested in.

基本上，此種資料可攜性之要素不僅為當事人提供了取得和再使用資料之能力，亦使其可就所提供之資料傳輸予另一服務提供商（無論是否在同一產業類別內）。除了透過賦予消費者權利以防止「被鎖在」某服務提供商，資料可攜權被預期可在當事人控制下，以安全可靠之方式促進創新及資料控管者間個人資料共享之機會[7]。資料可攜性可增進個人資料用戶在組織之間對個人資料在受控制的情形下進行有限之分享，從而豐富服務和客戶體驗[8]。在用戶感興趣的各種服務中，資料可攜性可促進相關用戶個人資料之傳輸和再使用。

- **Controllership**
  控制權

---

[5] See also section V.
請另參閱第V節。

[6] As a consequence, special attention should be paid to the format of the transmitted data, so as to guarantee that the data can be re-used, with little effort, by the data subject or another data controller. See also section V.
因此，應特別注意傳輸資料之格式，以確保當事人或其他資料控管者可輕鬆地重複使用資料。請另參閱第V節。

[7] See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France.
請參閱歐洲各項實驗應用程式，例如英國的MiData，法國FING的MesInfos / SelfData。

[8] The so-called quantified self and IoT industries have shown the benefit (and risks) of linking personal data from different aspects of an individual's life such as fitness, activity and calorie intake to deliver a more complete picture of an individual's life in a single file.
所謂的自我量化和物聯網產業已經顯示出將個人資料與個人生活不同面向（如健身、活動和卡路里攝取）相互連結之益處（和風險），以便在單一檔案中提供更完整之個人生活描述。

Data portability guarantees the right to receive personal data and to process them, according to the data subject's wishes[9].

資料可攜性確保當事人得依據其意願接收及運用個人資料之權利[9]。

Data controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data. They act on behalf of the data subject, including when the personal data are directly transmitted to another data controller. In this respect, the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient. At the same time the controller should set safeguards to ensure they genuinely act on the data subject's behalf. For example, they can establish procedures to ensure that the type of personal data transmitted are indeed those that the data subject wants to transmit. This could be done by obtaining confirmation from the data subject either before transmission or earlier on when the original consent for processing is given or the contract is finalised.

資料控管者在依據第20條規定之要件回應資料攜帶請求時，控管者不需對當事人或接收個資之另一家公司就該資料之運用負責。資料控管者代表當事人行事，包括將個人資料直接傳輸至另一資料控管者。在此情況下，考量到接收方並非傳輸資料之控管者所選擇，因此該資料控管者無法負責接收資料控管者對資料保護法之遵循。同時，控管者應設置安全維護措施，以確保其確實代表當事人行事。例如，控管者可建立程序以確保傳輸之個人資料類型確實為當事人所欲傳輸之資料。此程序可透過在傳輸前、在最初給予運用同意時、或於成立契約時獲得當事人之確認來完成。

Data controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it. Of course, these data should already be accurate, and up to date, according to the principles stated in Art 5(1) of the GDPR. Moreover, data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period[10]. Importantly, there is no additional requirement to retain data beyond the otherwise applicable retention periods, simply to serve any potential future data portability request.

回應資料攜帶請求之資料控管者並無傳輸資料前檢查和驗證資料品質之特定義務。當然，依據GDPR第5條第1項規定之原則，這些資料應已是正確且最新的。此外，資料可攜性並未規定資料控管者有義務保留個人資料超過必要時間或超過任何指定的保留期限[10]。重要

[9] The right to data portability is not limited to personal data that are useful and relevant for similar services provided by competitors of the data controller.

資料可攜權不限於只針對與資料控管者提供類似服務之競爭者提供有用且相關之個人資料。

[10] In the example above, if the data controller does not retain a record of songs played by a user then this personal data cannot be included within a data portability request.

作為上述示例，若資料控管者並無保留用戶播放歌曲之記錄，則該個人資料不應包含在資料攜帶請求中。

的是，並未額外要求資料保留超出其所適用之保留期限，僅為提供任何未來可能之資料攜帶請求。

Where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist "the controller by appropriate technical and organisational measures, (…) to respond to requests for exercising the data subject's rights". The data controller should therefore implement specific procedures in cooperation with its data processors to answer data portability requests. In case of a joint controllership, a contract should allocate clearly the responsibilities between each data controller regarding the processing of data portability requests.
若所請求之個人資料係由資料受託運用者所運用，依據GDPR第28條所簽訂之契約必須包括有義務「透過適當技術性和組織性措施協助控管者，（...）以回應當事人行使其權利之請求」。因此，資料控管者應與其資料受託運用者合作執行特定程序，以回應資料攜帶之請求。在共同控管之情況下，契約應明確分配各個資料控管者間關於處理資料攜帶請求之責任。

In addition, a receiving data controller[11] is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing. For example, in the case of a data portability request made to a webmail service, where the request is used by the data subject to obtain emails and send them to a secured archive platform, the new data controller does not need to process the contact details of the data subject's correspondents. If this information is not relevant with regard to the purpose of the new processing, it should not be kept and processed. In any case, receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request. Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once they have been labelled for the purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.
此外，接收資料控管者[11]需負責確保被提供之可攜資料在新的資料運用上係相關且非過多的。例如，在向網路郵件服務者提出資料攜帶請求之情況下，當事人利用該請求以獲取電子郵件並將其發送至安全的歸檔備份平台，新的資料控管者不需運用當事人通訊聯絡人之詳細資訊。若此資訊與新的運用目的並無關聯，則不應保留和運用該資訊。在任何情況下，接收資料控管者並無義務接受和運用依資料攜帶請求傳輸過來之個人資料。同樣的，若當事人請求將其銀行交易之詳細資訊傳輸至提供協助管理財務之服務，一旦該資料為提供新

[11] i.e. that receives personal data following a data portability request made by the data subject to another data controller.
即依當事人資料攜帶請求接收個人資料之另一資料控管者。

服務之目的而標籤化，則接收資料控管者不需接受所有資料或保留所有交易詳細資訊。易言之，被接受和保留之資料應僅限於接收資料控管者為提供服務所必需和相關之資料。

A “receiving” organization becomes a new data controller regarding these personal data and must respect the principles stated in Article 5 of the GDPR. Therefore, the ”new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14[12]. As for any other data processing performed under its responsibility, the data controller should apply the principles laid down in Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, storage limitation and accountability[13].

「接收」資料的組織成為這些個人資料之新資料控管者，且必須遵守GDPR第5條中規定之原則。因此，「新的」接收資料控管者必須依據第14條規定之透明化要求，在回應任何可攜資料傳輸請求前，清楚且直接地說明新的運用目的[12]。對於在其責任範圍內進行的任何其他資料運用，資料控管者應遵守第5條規定之原則，如合法性、公正性和透明化、目的限制性、資料最小化、準確性、完整性和機密性、儲存限制和課責性[13]。

Data controllers holding personal data should be prepared to facilitate their data subject’s right to data portability. Data controllers can also choose to accept data from a data subject, but are not obliged to.

持有個人資料之資料控管者應就協助其當事人行使資料可攜權有所準備。資料控管者亦可選擇，但無義務，接受來自當事人之資料。

- **Data portability vs. other rights of data subjects**
  資料可攜性 vs. 當事人之其他權利

When an individual exercises his or her right to data portability he or she does so without prejudice to any other right (as is the case with any other rights in the GDPR). A data subject can continue to use and benefit from the data controller’s service even after a data portability operation. Data portability does not automatically trigger the erasure of the data[14] from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted. The data subject can exercise his or her rights as long

[12] In addition, the new data controller should not process personal data, which are not relevant, and the processing must be limited to what is necessary for the new purposes, even if the personal data are part of a more global data-set transmitted through a portability process. Personal data, which are not necessary to achieve the purpose of the new processing, should be deleted as soon as possible.
此外，新的資料控管者不得運用不相關之個人資料，且運用必須限於為新目的所必需，即使透過攜帶性程序傳輸之個人資料屬於更整體性資料集之一部分。非為實現新的運用目的所必需之個人資料應盡快刪除。

[13] Once received by the data controller, the personal data sent as part of the right to data portability can be considered as “provided by” the data subject and be re-transmitted according to the right to data portability, to the extent that the other conditions applicable to this right (ie. the legal basis of the processing, …) are met.
作為資料可攜權之一部分而被傳輸之個人資料，一旦被資料控管者接收，即可被視為「由當事人提供」。若適用於資料可攜權之其他法律要件（即運用之法律基礎，.....）得到滿足，並可依據資料可攜權再傳輸。

as the data controller is still processing the data.

當個人行使其資料可攜權時，此行為並不影響該當事人任何其他權利（如同GDPR中的任何其他權利）。即使在資料可攜性作業後，當事人亦可繼續使用資料控管者之服務並從中受益。資料可攜性不會自動觸發從資料控管者系統中移除資料[14]，亦不會影響適用於已傳輸資料之原始保存期。只要資料控管者仍繼續運用該資料，當事人即可行使其權利。

Equally, if the data subject wants to exercise his or her right to erasure ("right to be forgotten" under Article 17), data portability cannot be used by a data controller as a way of delaying or refusing such erasure.

同樣的，若當事人欲行使其刪除權（第17條規定之「被遺忘權」），資料控管者不得將資料可攜性作為延遲或拒絕此類刪除之方式。

Should a data subject discover that personal data requested under the right to data portability does not fully address his or her request, any further request for personal data under a right of access should be fully complied with, in accordance with Article 15 of the GDPR.

若當事人發現依據資料可攜權請求之個人資料未能完全滿足其請求時，依據GDPR第15條，當事人基於近用權所為之任何進一步個人資料請求皆須被完全遵從。

Furthermore, where a specific European or Member State law in another field also provides for some form of portability of the data concerned, the conditions laid down in these specific laws must also be taken into account when satisfying a data portability request under the GDPR. First, if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation only, then the GDPR's data portability provisions will not apply to this request[15]. If, on the other hand, the request is aimed at portability under the GDPR, the existence of such specific legislation does not override the general application of the data portability principle to any data controller, as provided by the GDPR. Instead, it must be assessed, on a case by case basis, how, if at all, such specific legislation may affect the right to data portability.

此外，當某一特定歐盟或其成員國法律於其他領域中就相關資料亦提供了某種形式之可攜帶性，在滿足GDPR下之資料攜帶請求時，亦須考量這些特定法律規定之要件。一方面，若當事人之要求明確表示其意圖並非行使GDPR中之權利，而僅係依據某特定領域之法律行使權利，則GDPR的資料可攜性條款將不適用於該請求[15]。另一方面，若請求之目的係針對GDPR下之可攜性，則此種特定法律之存在並不會優先於GDPR所規定的對任何資料

[14] as stated in Article 17 of the GDPR
如GDPR第17條所述。

[15] For example, if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive.
例如，若當事人之請求係針對向帳戶資訊服務提供商提供對其銀行帳戶過往記錄之存取，則基於支付服務指令2（PSD2）中所述之目的，應依據該指令之規定授予此類存取之權限。

控管者就資料可攜性原則之一般適用。相反的，必須依據具體情況逐案評估這些特定法律如何影響資料可攜性。

III. When does data portability apply?
何時適用資料可攜性？

- **Which processing operations are covered by the right to data portability?**
  資料可攜權涵蓋何種運用作業？

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data.
GDPR合規性要求資料控管者須具有運用個人資料之明確法律基礎。

In accordance with Article 20(1)(a) of the GDPR, **in order to fall under the scope of data** portability, processing operations must be based:
依據GDPR第20條第1項第a款，**為落入資料可攜性之範圍內**，運用作業必須基於：

- either on the data subject's consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data);
  當事人之同意（依據第6條第1項第a款，或依據第9條第2項第a款，當涉及特殊類型之個人資料時）；

- or, on a contract to which the data subject is a party pursuant to Article 6(1)(b).
  或當事人為締約方之契約（依據第6條第1項第b款）。

As an example, the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party.
例如，當事人從網路書店所購買書籍之書名，或透過音樂串流媒體服務收聽之歌曲通常是在資料可攜性範圍內之個人資料示例，因其係基於履行當事人為締約方之契約所為之運用。

The GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract[16]. For example, there is no obligation for financial institutions to answer a data portability request concerning personal data processed as part of their obligations obligation to prevent and detect money laundering and other financial crimes; equally, data portability does not cover professional contact details processed in a business to business relationship in cases where the processing is neither based on the consent of the data subject nor on a contract to which he or she is a party.

當個人資料之運用非基於同意或契約之情況下，GDPR並未建立資料可攜性之一般權利[16]。例如，作為防止和偵查洗錢及其他金融犯罪義務之一部分所為之資料運用，金融機構並無義務回應有關此類個人資料之資料攜帶請求；同樣的，當運用既非基於當事人之同意，亦非基於當事人為契約締約方之情況下，資料可攜性不涵蓋企業對企業關係中所運用之職業聯絡明細。

When it comes to employees' data, the right to data portability typically applies only if the processing is based on a contract to which the data subject is a party. In many cases, consent will not be considered freely given in this context, due to the imbalance of power between the employer and employee[17]. Some HR processings instead are based on the legal ground of legitimate interest, or are necessary for compliance with specific legal obligations in the field of employment. In practice, the right to data portability in an HR context will undoubtedly concern some processing operations (such as pay and compensation services, internal recruitment) but in many other situations a case by case approach will be needed to verify whether all conditions applying to the right to data portability are met.

當涉及員工資料時，資料可攜權通常僅適用於基於當事人為締約方之契約的運用情形。在許多情況下，由於雇主和員工之間的權力不對等，同意將無法被視為係自由給予的[17]。某些人力資源之運用係基於正當利益之法律依據，或係為遵守就業領域中之特定法律義務所必需。實務上，人力資源背景下之資料可攜權無疑將涉及某些運用作業（例如薪資、補償服務和內部招聘），但在許多其他情況下，須以個案方式來驗證是否所有適用於資料可攜權之要件皆被滿足。

Finally, the right to data portability only applies if the data processing is "carried out by automated means", and therefore does not cover most paper files.

最後，資料可攜權僅適用於當資料運用係「透過自動化方式執行」時，因此大多數的書面檔案不涵蓋在內。

---

[16] See recital 68 and Article 20(3) of the GDPR. Article 20(3) and Recital 68 provide that data portability does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation. Therefore, there is no obligation for data controllers to provide for portability in these cases. However, it is a good practice to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings. For data portability as a good practice in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217).

請參閱GDPR前言第68點和第20條第3項。第20條第3項和前言第68點規定，資料可攜性不適用於當資料運用係為執行公共利益之任務或行使資料控管者被賦與之官方權限所必需時，抑或當資料控管者正在履行其公務職責或遵守法律義務。因此，在這些情況下，資料控管者並無義務提供可攜性。然而，透過遵守管理資料可攜權之原則，建立自動回應資料攜帶請求之程序是一種優良實務做法。此方面之示例為政府服務提供可輕鬆下載過去個人所得稅申報表。當運用之法律依據係基於正當利益和現有自願性計劃所必須時，資料可攜性之優良實務做法請參閱29條工作小組第6/2014號意見第47和48頁關於正當利益的部分（WP217）。

[17] As the WP29 outlined in its Opinion 8/2001 of 13 September 2001 (WP48).

如29條工作小組在2001年9月13日的第8/2001號意見（WP48）中所述。

- **What personal data must be included?**
  必須包含何種個人資料？

Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be:
根據第20條第1項，在資料可攜權範圍內，資料必須是：

- personal data concerning him or her, and
  與當事人相關之個人資料，及
- which he or she has *provided* to a data controller.
  由當事人*提供*予資料控管者之個人資料。

Article 20(4) also states that compliance with this right shall not adversely affect the rights and freedoms of others.
第20條第4項亦規定，對此一權利之遵守不得對他人之權利和自由產生不利影響。

First condition: personal data concerning the data subject
第一項要件：與當事人相關之個人資料

Only personal data is in scope of a data portability request. Therefore, any data that is anonymous[18] or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is within the scope.
僅有個人資料屬於資料攜帶請求之範圍內。因此，任何匿名[18]或與當事人無關之資料皆不在此範圍內。然而，可清楚與當事人連結之假名化資料（例如，由當事人提供相對應之識別資訊，請參閱第11條第2項）則屬於此範圍內。

In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition).
在許多情況下，資料控管者會運用包含數個當事人個人資料之資訊。在此情況下，資料控

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

管者不應對「與當事人相關之個人資料」一詞採取過度限縮之解釋。例如，電話、個人間通訊或網路電話（VoIP）之記錄可包括（在用戶帳戶歷史中）來電或去電第三方之資訊細節。雖然該記錄包含相關數個當事人之個人資料，但用戶應仍能夠依資料攜帶請求取得這些記錄，因該記錄（亦）與該當事人相關。然而，若這些記錄隨後被傳輸至新的資料控管者，則新的資料控管者運用該資料之任何目的不得對第三方之權利和自由產生不利影響（請參閱下文：第三項要件）。

Second condition: data provided by the data subject

第二項要件：由當事人提供之資料

The second condition narrows the scope to data "provided by" the data subject.

第二項要件將範圍限縮至由當事人「提供」之資料。

There are many examples of personal data, which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data "provided by" the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, "provided by" should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects[19], activity logs, history of website usage or search activities.

有許多個人資料係由當事人有意識且積極「提供」之示例，例如透過網路表格提交之帳戶資料（例如郵件地址、用戶名稱、年齡）。然而，觀察其活動所得之資料亦屬由當事人「提供」之資料。因此，29條工作小組認為，為充分發揮此項新權利之價值，「提供」亦應包括從用戶活動中觀察到的個人資料，如智慧型電錶所運用之原始資料或其他類型之連結物件[19]、活動日誌、網站使用或搜尋活動的歷史記錄。

This latter category of data does not include data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected.

後者資料種類不包括由資料控管者創建之資料（使用觀察到或直接輸入提供之資料），例如透過分析所蒐集之原始智慧型電錶資料而創建之用戶檔案。

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

[19] By being able to retrieve the data resulting from observation of his or her activity, the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected.

透過取得觀察其活動所產生之資料，當事人亦將能夠更佳地了解資料控管者對觀察資料範圍之執行選擇，並將處於更佳之地位選擇願意提供何種資料以獲得類似之服務，且可了解其隱私權在何種程度上受到尊重。

依據其來源可區分為不同類型之資料，從而確認其是否屬於資料可攜權之範圍。以下資料類型可被視為「由當事人提供」：

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)
  當事人積極且有意識提供之資料（例如郵件地址、用戶名稱、年齡等）

- **Observed data provided by the data subject by virtue of the use of the service or the device**. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.
  經由使用服務或設備而由當事人提供之觀察資料。此類型資料可包括例如個人搜尋歷史、流量資料和位置資料。其亦可包括其他原始資料，例如由穿戴式裝置所追蹤之心跳。

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right[20].
相反者為由資料控管者基於「由當事人提供」之資料所創建之推論資料和衍生資料。例如，關於用戶健康狀況評估之結果，或在風險管理和財務法規背景下創建之檔案（例如，給予信用評分或遵守反洗錢法規）不得被視為由當事人「所提供」。即使此類資料可能係資料控管者所存留檔案之一部分，並且係透過當事人所提供之資料分析推論或衍生而來（例如透過當事人之行為），這些資料通常不會被視為「由當事人提供」，因此不屬於此項新權利之範圍[20]。

In general, given the policy objectives of the right to data portability, the term "provided by the data subject" must be interpreted broadly, and should exclude "inferred data" and "derived data",

[20] Nevertheless, the data subject can still use his or her "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" as well as information about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject", according to Article 15 of the GDPR (which refers to the right of access).
然而，當事人仍可行使其「從控管者取得關於是否正在運用與當事人相關個人資料之確認的權利，並且在這種情況下，得近用個人資料」，以及關於「第 22 條第 1 項和第 4 項所提及自動化決策 （包含剖析）之存在，以及至少於這些情況下，依據 GDPR 第 15 條（涉及近用權）規定，取得關於所涉邏輯，以及這些資料之運用會對當事人造成之重大和預計之後果之有意義資訊」。

which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller[21].
一般而言，鑑於資料可攜權之政策目的，「由當事人提供」一詞必須做廣義之解釋，並應排除「推論資料」和「衍生資料」，此包括由服務提供者創建之個人資料（例如，演算法之結果）。資料控管者可排除這些推論資料，但應包含當事人透過控管者所提供之技術方式而提供的所有其他個人資料[21]。

Thus, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.
因此，「由...提供」一詞包括與當事人活動相關之個人資料或由觀察個人行為所得之結果，但不包括由該行為之後續分析產生之資料。相反的，任何由資料控管者作為資料運用之一部分而創建的個人資料（例如透過個人化或推薦程序、透過用戶分類或剖析），是由當事人提供之個人資料衍生或推論而來，並不屬於資料可攜權之範圍。

Third condition: the right to data portability shall not adversely affect the rights and freedoms of others
第三項要件：資料可攜權不應對他人之權利和自由產生不利影響

With respect to personal data concerning other data subjects:
與其他當事人相關之個人資料：

The third condition is intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR)[22].
第三項要件旨在避免取得和傳輸包含其他（未經同意）當事人之個人資料至新的資料控管者，當這些資料之運用方式可能會對該其他當事人之權利和自由產生不利影響（GDPR第

[21] This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as "provided by" him or her even if the data are not actively or consciously transmitted.
此包括基於資料蒐集目的，在活動期間觀察到與當事人相關之所有資料，例如交易歷史或存取記錄。透過追蹤和記錄當事人而蒐集之資料（例如記錄心跳之應用程式或用於追蹤瀏覽行為之技術）亦應被視為「由當事人所提供」，即使該資料並非是被積極或有意識地傳輸。

20條第4項）[22]。

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).
例如，若從一資料控管者向另一資料控管者傳輸資料，將會阻止第三方行使其作為GDPR下當事人之權利（例如被告知權、近用權等）時，則會產生此種不利影響。

The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with that controller. Where personal data of third parties are included in the data set another legal basis for the processing must be identified. For example, a legitimate interest may be pursued by the data controller under Article 6(1)(f), in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity. The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller.
當事人經由給予新的資料控管者同意，或與該控管者簽訂契約，而開始傳輸其個人資料至另一資料控管者。若資料集包含第三方之個人資料，則必須確認資料運用的另一法律依據。例如，資料控管者可依據第6條第1項第f款尋求正當利益，尤其是當資料控管者之目的係向當事人提供服務，而該服務允許後者為純粹的個人或家庭活動運用個人資料。在涉及並可能影響第三方的個人活動環境中，若資料控管者無法以任何方式決定此種運用，則此由當事人發起之運用作業仍應由該當事人負責。

For example, a webmail service may allow the creation of a directory of a data subject's contacts, friends, relatives, family and broader environment. Since these data relate to (and are created by) the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to that data subject.
例如，網路郵件服務可允許當事人建立其聯絡人、朋友、親戚、家庭和更廣泛情況之目錄。由於這些資料與希望行使資料可攜權之可識別當事人相關（並由其建立），資料控管者應將接收和傳送電子郵件的完整目錄傳輸予該當事人。

Similarly, a data subject's bank account can contain personal data relating to the transactions not

[22] Recital 68 provides that "where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation."
前言第68點規定「在某些個人資料集內，當涉及數個當事人之情況下，接收個人資料之權利不應影響其他當事人依據本規則享有之權利和自由。」

just of the account holder but also those of other individuals (e.g., if they have transferred money to the account holder). The rights and freedoms of those third parties are unlikely to be adversely affected by the transmission of the bank account information to the account holder once a portability request is made—provided that in both examples the data are used for the same purpose (i.e., a contact address only used by the data subject or a history of the data subject's bank account.

同樣的，當事人之銀行帳戶可包含涉及帳戶持有人以及與其他當事人相關之個人交易資料（例如，若其他當事人將金錢轉帳予帳戶持有人）。若帳戶持有人提出攜帶請求將銀行帳戶資訊傳輸予其本人，則不大可能對這些第三方之權利和自由產生不利影響 – 因在此兩個示例中，資料皆用於相同之目的（即僅由當事人使用之聯絡地址或當事人銀行帳戶的歷史紀錄。）

Conversely, the rights and freedoms of third parties will not be respected if the new data controller uses the personal data for other purposes, e.g. if the receiving data controller uses personal data of other individuals within the data subject's contact directory for marketing purposes.

相反的，若新的資料控管者將個人資料用於其他目的時，第三方之權利和自由將沒有受到尊重。例如，若接收資料控管者基於行銷目的使用當事人聯絡目錄中其他當事人之個人資料。

Therefore, to prevent adverse effects on the third parties involved, the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other third party data subjects. For example, this information should not be used to enrich the profile of the third party data subject and rebuild his social environment, without his knowledge and consent[23]. Neither can it be used to retrieve information about such third parties and create specific profiles, even if their personal data are already held by the data controller. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects.

因此，為防止對相關之第三方產生不利影響，僅有當資料係由用戶單獨控制且僅係針對個人或家庭需求進行管理時，始允許由另一資料控管者運用此類型之個人資料。接收資料之「新的」資料控管者（依用戶請求向其傳輸資料）不可將所傳輸之第三方資料用於其自身之目的，例如向其他第三方當事人提供貨品或服務行銷。例如，在未經第三方當事人知情

和同意之情況下，此資訊不應用於充實其檔案和重建其社交環境[23]。即便資料控管者已持有其個人資料，此資訊亦不得用於取得有關該第三方之資訊並用來創建特定檔案。否則，此種運用可能係非法且不公平，特別是若相關之第三方並未被告知且無法行使其作為當事人之權利時。

Furthermore, it is a leading practice for all data controllers (both the "sending" and "receiving" parties) to implement tools to enable data subjects to select the relevant data they wish to receive and transmit and exclude, where relevant, data of other individuals. This will further assist in reducing the risks for third parties whose personal data may be ported.
此外，作爲優良實務做法，所有資料控管者（「傳輸」和「接收」方）都應建置工具使當事人得選擇其所希望接收和傳輸之相關資料，並在適當時排除其他當事人之資料。如此將進一步協助降低第三方個人資料可能被輸出之風險。

Additionally, the data controllers should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. if they also want to move their data to some other data controller. Such a situation might arise, for example, with social networks, but it is up to data controllers to decide on the leading practice to follow.
此外，資料控管者應為相關之其他當事人建置同意機制，以便在該當事人願意提供同意之情況下更容易為資料傳輸，例如若該當事人亦欲將其資料轉移至其他資料控管者。比方，社群網路就可能會出現此種情況，但遵循何種實務作法，由資料控管者決定。

With respect to data covered by intellectual property and trade secrets:
關於智慧財產和營業秘密所涵蓋之資料：

The rights and freedoms of others are mentioned in Article 20(4). While not directly related to portability, this can be understood as "including trade secrets or intellectual property and in particular the copyright protecting the software. However, even though these rights should be considered before answering a data portability request, "the result of those considerations should not be a refusal to provide all information to the data subject". Furthermore, the data controller should not reject a data portability request on the basis of the infringement of another contractual right (for example, an outstanding debt, or a trade conflict with the data subject).
第20條第4項提及了他人之權利和自由。雖然與可攜性並無直接關聯，但此可理解為「包含營業秘密或智慧財產權，尤其係保護軟體之著作權」。然而，即使在回應資料攜帶請求之前應考量這些權利，「不得以考量之結果拒絕向當事人提供所有資訊」。此外，資料控

[23] A social networking service should not enrich the profile of its members by using personal data transmitted by a data subject as part of his right to data portability, without respecting the principle of transparency and also making sure they rely on an appropriate legal basis regarding this specific processing.
若無法尊重透明化原則並確保特定運用係基於適當法律依據，社群網路服務不應透過使用當事人行使其資料可攜權而傳輸之個人資料以充實其會員檔案。

管者不應基於侵害另一契約權利（例如未清償債務或與當事人之交易衝突）拒絕資料攜帶之請求。

The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights.
當資訊之使用方式可能被視為不公平，或構成對智慧財產權之侵犯時，資料可攜權即非當事人得濫用資訊之權利。

A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.
然而，潛在之商業風險本身不可作為拒絕回應資料攜帶請求之基礎，且資料控管者得以不洩露營業秘密或智慧財產權資訊之形式傳輸由當事人提供之個人資料。

IV. How do the general rules governing the exercise of data subject rights apply to data portability?
規範行使當事人權利之一般規則如何適用於資料可攜性？

- **What prior information should be provided to the data subject?**
  應向當事人提供何種前置資訊？

In order to comply with the new right to data portability, data controllers must inform data subjects of the existence of the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen "at the time where personal data are obtained". If the personal data have not been obtained from the data subject, the data controller must provide the information as required by Articles 13(2)(b) and 14(2)(c).
為符合新的資料可攜權，資料控管者必須告知當事人此項新的資料可攜權之存在。若直接從當事人處蒐集相關之個人資料，則必須「在獲得個人資料時」告知。若非從當事人處獲得個人資料，則資料控管者必須提供第13條第2項第b款和14條第2項第c款要求之資訊。

"Where the personal data have not been obtained from the data subject", Article 14(3) requires the information to be provided within a reasonable time not exceeding one month after obtaining the data, during first communication with the data subject, or when disclosure is made to third parties[24].
「若非從當事人處獲得個人資料」，第14條第3項規定資訊必須在下列情況下提供：獲得資料後之一個月內的合理時間、在與當事人進行首次溝通時、或在向第三方揭露時[24]。

[24] Article 12 requires that data controllers provide "any communications […] in a concise, transparent, intelligible,

When providing the required information data controllers must ensure that they distinguish the right to data portability from other rights. Therefore, WP29 recommends in particular that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.
在提供所需資訊時，資料控管者必須確保其將資料可攜權與其他權利有所區分。因此， 29條工作小組特別建議資料控管者清楚地解釋，當事人透過近用權和資料可攜權得接收之資料類型間之差異。

In addition, the Working Party recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated.
此外，工作小組也建議資料控管者在當事人關閉其可能擁有之任何帳戶前，提供包含有關資料可攜權之資訊。如此將允許用戶盤點評估其個人資料，並在契約終止前可輕鬆地將資料傳輸至自身之裝置或另一個提供者。

Finally, as leading practice for "receiving" data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services. In addition to underpinning fair processing, this allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.
最後，作為「接收」資料控管者的主要實務做法，29條工作小組建議向當事人提供與執行服務相關個人資料性質的完整資訊。除了加強公平運用之基礎外，此做法亦限縮用戶造成對第三方之風險，以及任何其他非必要個人資料之複製，即使該複製並未涉及其他當事人。

- **How can the data controller identify the data subject before answering his request?**
  在回應請求前，資料控管者如何識別當事人？

There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights (including the right to data portability) unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. However, as per Article 11(2), in such circumstances the data subject can provide more

---

and easily assessable form, using clear and plain language, in particular for any information addressed specifically to a child."
第12條規定資料控管者提供之「任何溝通[…]需以簡明、透明、易懂和易於評估之形式為之並使用清晰簡潔之語言，尤其係專門針對兒童之任何資訊。」

information to enable his or her identification. Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. Where a data subject provides additional information enabling his or her identification, the data controller shall not refuse to act on the request. Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

在GDPR中並無關於如何認證當事人之法定要求。然而，GDPR第12條第2項規定，除非控管者運用個人資料之目的不需識別當事人，且其可證明無法識別該當事人，否則資料控管者不得拒絕當事人行使其權利（包括資料可攜權）之請求。然而，依據第11條第2項，在此種情況下，當事人可提供更多資訊以便識別其身分。此外，第12條第6項規定，若資料控管者對當事人身分有合理的懷疑時，可要求提供進一步資訊以確認當事人身分。若當事人提供得識別其身分之額外資訊時，資料控管者不得拒絕對該請求採取行動。當線上蒐集之資訊和資料與假名化或特殊標識相連結時，資料控管者即可執行適當程序，以使當事人能夠提出資料攜帶請求並接收與其相關之資料。無論如何，資料控管者必須執行認證程序，以加強確認請求其個人資料或一般性行使GDPR權利之當事人身分。

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes[25].

這些程序通常已經存在。在與其簽訂契約或取得對運用之同意前，資料控管者通常已對當事人進行了認證。因此，用於註冊之與運用相關的當事人個人資料亦可做為證據，以便為可攜性之目的驗證當事人[25]。

While in these cases, the data subjects' prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

[25] For example, when the data processing is linked to a user account, providing the relevant login and password might be sufficient to identify the data subject.
例如，當資料運用連結至用戶帳戶時，提供相關之登錄名稱和密碼可能足以識別當事人。

雖然在這些情況下，當事人事前之身分識別可能需要請求其提供合法身分證明，但這種認證可能與評估資料和相關個人間之連結性無關，因為此類連結性與正式或合法身分並無關聯。基本上，資料控管者請求額外資訊以評估當事人身分之能力，不得導致過多之要求，和導致蒐集與強化個人和所請求個人資料間之連結無關或不必要之個人資料。

In many cases, such authentication procedures are already in place. For example, usernames and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity.
在許多情況下，此種認證程序已經存在。例如，用戶名稱和密碼通常用於允許當事人存取其電子郵件帳戶、社群網路帳戶和用於各種其他服務之帳戶，而對於某些帳戶之使用，當事人會選擇不透露其全名和身分。

If the size of data requested by the data subject makes transmission via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request[26], the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media or allowing for the personal data to be transmitted directly to another data controller (as per Article 20(2) of the GDPR where technically feasible).
若當事人請求之資料大小在使用網路傳輸時會造成問題，資料控管者與其可能容許最長三個月的延長期限以遵循請求[26]，不如考量以替代方式提供資料，例如使用串流傳輸或儲存到CD、DVD或其他實體媒介，或允許個人資料直接傳輸至另一資料控管者（依據GDPR第20條第2項當技術可行時）。

- **What is the time limit imposed to answer a portability request?**
  回應可攜性請求之時間限制為何？

Article 12(3) requires that the data controller provides "information on action taken" to the data subject "without undue delay" and in any event "within one month of receipt of the request". This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.
第12條第3項要求資料控管者向當事人「告知所欲採取之行動」，「不得無故延遲」，且無論如何，「在收到請求後的一個月內」為之。對於複雜案件，此一個月之期限最多可延長至三個月，前提是當事人已於原始請求的一個月內被告知此類延遲之原因。

Data controllers operating information society services are likely to be better equipped to be able

[26] Article 12(3): "The controller shall provide information on action taken on a request".
第12條第3項：「控管者應提供對請求所欲採取行動之資訊」。

to comply with requests within a very short time period. To meet user expectations, it is a good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects.
經營資訊社群服務之資料控管者可能有較佳之能力，能夠在很短的時間內遵循請求。為了滿足用戶的期待，明確界定通常可回應資料攜帶請求之時間範圍，並將其傳達予當事人，為優良實務做法。

Data controllers who refuse to answer a portability request shall, pursuant to Article 12(4), inform the data subject "the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy", no later than one month after receiving the request.
拒絕回應攜帶請求之資料控管者應依據第12條第4項，於收到請求後的一個月內，通知當事人「不採取行動之原因以及可向監管機關提出申訴和尋求司法救濟之可能性」。

Data controllers must respect the obligation to respond within the given terms, even if it concerns a refusal. In other words, the data controller cannot remain silent when it is asked to answer a data portability request.
資料控管者必須尊重在規定時間內作出回應之義務，即便是拒絕。易言之，當資料控管者被要求就資料攜帶請求做出回應時，不得保持沉默。

- **In which cases can a data portability request be rejected or a fee charged?**
  於何種情況下可拒絕資料攜帶的請求或收取費用？

Article 12 prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, "in particular because of their repetitive character". For information society services that specialise in automated processing of personal data, implementing automated systems such as Application Programming Interfaces (APIs)[27] can facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests. Therefore, there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.
第12條禁止資料控管者為提供個人資料收取費用，除非資料控管者得證明請求明顯無依據或過度，「尤其是因為具有重複性」。對於擅長於自動化運用個人資料之資訊社群服務，執行諸如應用程式介面（API）[27]之類的自動化系統可促進與當事人間之交換，因而減少了因重複請求導致的潛在負擔。因此，即使對於多個資料攜帶請求，資料控管者極少能夠證明拒絕提供請求資訊有正當理由。

[27] Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems.
應用程式介面（API）係指資料控管者提供之應用程式或網頁服務介面，以便其他系統或應用程式可連結和使用其系統。

In addition, the overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request. In fact, Article 12 of the GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller. As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.
此外，為回應資料攜帶請求而建立之程序總成本不應在決定請求是否過度時列為考量。事實上，GDPR第12條係針對單一當事人所提出之請求，而非資料控管者收到的請求總數量。因此，整體系統執行成本既不應向當事人收取費用，亦不應用於證明拒絕回應可攜性請求具有正當理由。

V. How must the portable data be provided?
如何提供可攜資料？

- **What are the expected means the data controller should implement for data provision?**
  資料控管者為提供資料所應執行之預期方式為何?

Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided.
GDPR第20條第1項規定，當事人有權利將資料傳輸至另一控管者，而不受其提供個人資料之控管者所阻礙。

Such hindrance can be characterised as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. For example, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands[28].
此種阻礙可表徵為資料控管者為阻止或減慢當事人或其他資料控管者之存取、傳輸或再使用而設置之任何法律、技術或財務障礙。例如，此種阻礙可能為：要求傳輸資料之費用、缺乏資料格式或API或所提供格式之互通性或可存取性、取得完整資料集之過度延遲或複雜性、故意模糊資料集、或特殊和不當或過度的產業標準化或認證要求[28]。

[28] Some legitimate obstacles might arise, as the ones, which are related to the rights and freedoms of others mentioned in Article 20(4), or the ones that relate to the security of the controllers' own systems. It shall be the responsibility of the data controller to justify why such obstacles would be legitimate and why they do not constitute a hindrance in the meaning of Article 20(1).
某些合法障礙可能存在，如與第 20 條第 4 項中所提及他人之權利和自由相關之障礙，或與控管者自身系統安全相關之障礙。資料控管者有責任證明為何這些障礙係合法的，以及為何不構成第 20 條第 1 項中之阻礙。

Article 20(2) also places obligations on data controllers for transmitting the portable data directly to other data controllers "when technically feasible".
第20條第2項亦規定了資料控管者「在技術上可行時」有直接將可攜資料傳輸予其他資料控管者之義務。

The technical feasibility of transmission from data controller to data controller, under the control of the data subject, should be assessed on a case by case basis. Recital 68 further clarifies the limits of what is "technically feasible", indicating that "it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".
在當事人控制下，從一資料控管者傳輸至另一資料控管者之技術可行性，應依據個案具體情況進行評估。前言第68點進一步闡明「技術上可行」之限制，並指出「不應要求控管者有義務採行或維護技術上相容之運用系統」。

Data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way[29], and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject's request (Article 12(4)).
資料控管者被期待能以可互通之格式傳輸個人資料，即便其他資料控管者並未被課以支援這些格式之義務。因此，當兩個系統之間的安全通訊[29]為可行，以及當接收系統在技術上處於可接收輸入資料之狀態，即可將資料從一資料控管者直接傳輸至另一資料控管者。若因技術障礙禁止直接傳輸，資料控管者應向當事人解釋這些障礙，否則將與拒絕依當事人請求採取行動的決定相類似（第12條第4項）。

On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:
在技術性層面上，為了對當事人或其他資料控管者提供可攜資料，資料控管者應研究和評估兩種不同且互補之方式：

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
  直接傳輸可攜資料之整體資料集（或全部資料集之數項摘錄）；

- an automated tool that allows extraction of relevant data.

[29] Through an authenticated communication with the necessary level of data encryption.
透過具有必要等級資料加密之驗證通訊。

允許提取相關資料之自動化工具。

The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimising risk, and possibly allows for use of data synchronisation mechanisms[30] (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the "new" data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller.

在涉及複雜和大量資料集之情況下，資料控管者可能傾向選擇第二種方式，因該方式允許當事人在其請求之背景下，提取與其相關資料集之任何部分，且有助於風險最小化，並可能允許使用資料同步機制[30]（例如，在資料控管者間正常之通訊情境下）。此方式可能是確保「新的」資料控管者合規性的較佳方式，且在原始資料控管者方面，可做為降低隱私風險之優良實務做法。

These two different and possibly complementary ways of providing relevant portable data could be implemented by making data available through various means such as, for example, secured messaging, an SFTP server, a secured WebAPI or WebPortal. Data subjects should be enabled to make use of a personal data store, personal information management system[31] or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required.

為提供相關可攜資料，這兩種不同且可能互補之方式得透過各種方式執行以取得資料，例如，安全訊息傳遞、SFTP伺服器、安全WebAPI或WebPortal。應使當事人能夠利用個人資料儲存、個人資訊管理系統[31]或其他類型可信任之第三方，以持有和儲存個人資料，並授權資料控管者依據請求存取和運用個人資料。

- **What is the expected data format?**
  預期之資料格式為何？

The GDPR places requirements on data controllers to provide the personal data requested by the individual in a format, which supports re-use. Specifically, Article 20(1) of the GDPR states that the personal data must be provided "in a structured, commonly used and machine-readable

[30] Synchronisation mechanism can help reaching the general obligations under Article 5 obligation of the GDPR, which provides that "personal data shall be (…) accurate and, where necessary, kept up to date"
同步機制有助於實現 GDPR 第 5 條義務下之一般義務，該條款規定「個人資料應(…)準確，且在必要時隨時更新」。

[31] On personal information management systems (PIMS), see, for example, EDPS Opinion 9/2016, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf
有關個人資訊管理系統（PIMS），請參閱，例如EDPS第9/2016號意見：https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

format". Recital 68 provides a further clarification that this format should be interoperable, a term that is defined[32] in the EU as:
GDPR要求資料控管者以支援再使用之格式提供當事人所請求之個人資料。具體而言，GDPR第20條第1項規定，個人資料必須「以結構性、一般性和機器可讀性之格式」提供。前言第68點進一步闡釋了此種格式應可互通，互通一詞在歐盟被定義為[32]：

> *the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.*
> *有能力使迥然不同且多樣化之組織能夠藉由各自 ICT 系統之間的資料交換，透過其支援之業務程序，實現互利之共同目標，包括在各組織之間共享資訊和知識。*

The terms "structured", "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.
「結構性」、「一般性」和「機器可讀性」係促進資料控管者提供可互通資料格式之最低要求。也就是說，「結構性、一般性和機器可讀性」係就方法之描述，而互通性係所預期之結果。

Recital 21 of Directive 2013/37/EU[33,34] defines "machine readable" as:
第2013/37/EU號指令前言第21點[33,34]將「機器可讀性」定義為：

> *a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States*

---

[32] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20.
歐洲議會和理事會 2009 年 9 月 16 日第 922/2009/EC 號決議第 2 條，關於歐洲公共行政部門（ISA）之互通性解決方案 OJ L 260,03.10.2009，p.20。
[33]Amending Directive 2003/98/EC on the re-use of public sector information.
修訂第2003/98/EC號指令關於重複使用公眾部門資訊。
[34] The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as *machine-readable, interoperability*, *open format*, *standard*, *metadata*.
歐盟術語表（http://eur-lex.europa.eu/eli-register/glossary.html）進一步闡明了與本指引中所使用概念相關之期待，例如*機器可讀性、互通性、開放格式、標準、詮釋資料。*

should where appropriate encourage the use of open, machine-readable formats.
使軟體應用程式可輕易識別、辨認和提取特定資料之結構化檔案格式，包括個別描述及其內部結構。以機器可讀之結構化格式編碼之檔案資料為機器可讀式資料。機器可讀格式可以是開放或專有的；且可以是正式或非正式的標準。以限制自動運用之文件格式編碼的檔案，因不得或不易從中提取資料，所以不應視為係機器可讀格式。成員國應酌情鼓勵使用開放、機器可讀之格式。

Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.
鑑於資料控管者潛在可運用的資料類型廣泛，GDPR並未對所需提供之個人資料格式提出具體建議。最合適之格式在不同產業之間亦會有所不同，且可能已有適當之格式存在，被選擇之格式應可達到得解釋之目的，並可為當事人提供很大程度之資料可攜性。因此，受到昂貴授權限制之格式將不被視為是適當之方式。

Recital 68 clarifies that "The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible." **Thus, portability aims to produce interoperable systems, not compatible systems**[35].
前言第68點闡釋「當事人傳輸或接收有關其個人資料之權利不應加諸控管者義務，去採行或維護技術上相容之運用系統。」**因此，可攜性之目的在產生可互通之系統，而非相容之系統**[35]。

Personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability, such as inferred data or data related to security of systems. In this way, data controllers are encouraged to identify beforehand data which are within the scope of portability in their own systems. This additional data processing will be considered as ancillary to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.

[35] ISO/IEC 2382-01 defines interoperability as follows: "The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."
ISO/IEC 2382-01 定義互通性如下：「可在各種功能單元間溝通、執行程序或傳輸資料之能力，且要求用戶僅須稍微或不須了解這些單元之獨特性質。」

提供個人資料之格式預期將以具高度抽象性的任何內部或專有格式為之。因此，資料可攜性意味著資料控管者另一層面的資料運用，以便從其平台提取資料並過濾可攜性範圍外之個人資料，例如推論資料或與系統安全性相關之資料。因此，鼓勵資料控管者事先識別其自身系統中可攜性範圍內之資料。此種額外的資料運用將被視為係主要資料運用之輔助運用，因其執行並非為達到資料控管者所定義之新目的。

Where no formats are in common use for a given industry or given context, **data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity**, while maintaining a high level of abstraction. As such, suitable metadata should be used in order to accurately describe the meaning of exchanged information. This metadata should be enough to make the function and reuse of the data possible but, of course, without revealing trade secrets. It is unlikely therefore that providing an individual with PDF versions of an email inbox would be sufficiently structured or descriptive to allow the inbox data to be easily re- used. Instead, the e-mail data should be provided in a format which preserves all the metadata, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this format would impact or hinder the individual's right to re-use the data. In cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data a clear explanation of the impact of the choice should be provided. However, processing additional metadata for the sole purpose that they might be needed or wanted to answer a data portability request poses no legitimate ground for such processing.

若在特定行業或特定環境中並無一般性之使用格式，**資料控管者在提供資料時應使用常用的開放性格式（例如XML，JSON，CSV，...）以及有用且可達到最佳區別性之詮釋資料(metadata)**，同時保持高度抽象性。因此，應使用合適的詮釋資料，以便準確地描述所交換資訊之含義。此詮釋資料應可使資料具功能性且可再使用，但當然不至洩露商業機密。因此，為個人提供電子郵件收件匣的PDF版本資料不太可能具有足夠的結構性或描述性，使收件匣之資料可輕易地再使用。相反的，應以保留所有詮釋資料之格式提供電子郵件資料，以便有效地再使用資料。因此，在選擇提供個人資料的資料格式時，資料控管者應考量該格式將如何影響或阻礙當事人再使用資料之權利。若資料控管者能夠提供當事人選擇其偏好之個人資料格式，亦應對選擇之影響提供清楚的解釋。然而，當運用額外詮釋資料之唯一目的係該額外詮釋資料可能會被需要以回應資料攜帶請求，此即非該運用之正當依據。

WP29 strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability. This challenge has also been addressed by the European Interoperability Framework (EIF) which has created an agreed

approach to interoperability for organizations that wish to jointly deliver public services. Within its scope of applicability, the framework specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices[36].

29條工作小組強烈鼓勵產業相關人員和同業公會在一套通用且可互通之標準和格式上協同作業，以符合資料可攜權之要求。歐洲互通框架（EIF）亦對此挑戰提出解決方案，為那些希望共同提供公共服務的組織建立了一套議定的互通方法。在其適用範圍內，該框架規定了一系列之一般要件，例如詞彙、概念、原則、政策、指引、建議、標準、規格和實務做法[36]。

- **How to deal with a large or complex personal data collection?**
  如何處理大量或複雜之個人資料蒐集？

The GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise that might create difficulties for data controllers or data subjects.

當大量資料之蒐集、複雜資料結構或其他技術性問題可能對資料控管者或當事人造成困難時，GDPR並未解釋如何解決就此種挑戰之因應方式。

However, in all cases, it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data that could be provided by the data controller. For instance, data could first be provided in a summarised form using dashboards allowing the data subject to port subsets of the personal data rather than the entirety. The data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (see Article 12(1)) of the GDPR) in such a way that data subject should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

然而，在所有情況下，當事人能夠完全理解資料控管者所提供個人資料之定義、概要和結構是至關重要的。例如，可先使用儀表板式的摘要形式提供資料，允許當事人可接收個人資料子集，而非整體資料。資料控管者應以「簡潔、透明、易懂且便於取得之形式，使用清晰、平易的語言文字」（請參閱GDPR第12條第1項）提供概述，使當事人可就既定目的而欲下載或傳輸至另一資料控管者之資料擁有明確資訊。例如，當事人應能夠使用軟體應用程式輕鬆識別、辨認和運用來自該程式之特定資料。

As referenced above, a practical way by which a data controller can answer requests for data

[36] Source : http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.
資料來源：http：//ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

portability may be by offering an appropriately secured and documented API. This may enable individuals to make requests of the data controller for their personal data via their own or third-party software or grant permission for others to so do on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an externally accessible API, it may also be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the data controller.

如上所述，資料控管者可回應資料攜帶請求之實務作法，可以是提供適當受保護且經記錄建檔之API。誠如GDPR第20條第2項所述，如此可使當事人能夠透過其自身或第三方軟體向資料控管者請求個人資料，或授權他人代表其為之（包括另一資料控管者）。透過外部可存取之API授予對資料的近用權限，亦可能提供更複雜的存取系統，使當事人能夠為完整下載或僅為包含自上次下載以來變更之增量函數進行後續資料請求，而不因該額外請求造成對資料控管者之負擔。

-How can portable data be secured?

如何保護可攜資料？

In general, data controllers should guarantee the "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" according to Article 5(1)(f) of the GDPR.

一般而言，資料控管者應依據GDPR第5條第1項第f款之規定，確保「適當的個人資料安全，並使用適當技術性或組織性措施，防止包括未經授權或非法運用，以及防止意外遺失、破壞或損毀」。

However, the transmission of personal data to the data subject may also raise some security issues:

然而，將個人資料傳輸予當事人亦可能會引發某些安全疑慮：

How can data controllers ensure that personal data are securely delivered to the right person?

資料控管者如何確保個人資料安全地傳輸予合適之人？

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller is responsible for taking all the security measures needed to ensure not only that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect the personal data that remains in their systems, as well

as transparent procedures for dealing with possible data breaches[37]. As such, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures.

由於資料可攜性之目的係從資料控管者之資訊系統中獲取個人資料，因此傳輸成為這些相關資料之可能風險來源（尤其是在傳輸期間之資料侵害）。資料控管者有責任採取所有必要的安全措施，不僅須確保安全地傳輸個人資料（透過使用端對端或資料加密）至正確目的地（透過使用強力認證措施），亦須繼續保護仍存留於其系統中之個人資料，以及確保能因應潛在資料侵害的透明程序[37]。因此，資料控管者應評估與資料可攜性相關之特定風險，並採取適當之降低風險措施。

Such risk mitigation measures could include: if the data subject already needs to be authenticated, using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token- based authentications, should be used.

此類降低風險措施可包括：若當事人已需進行身分驗證，則使用附加的身分驗證資訊（如共用密碼）或其他身分驗證元素（如一次性密碼）；若懷疑帳戶已被盜用，則暫停或凍結傳輸；在從資料控管者直接傳輸至另一資料控管者之情況下，應強制使用授權驗證，例如token-based驗證。

Such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.

此類安全措施不得具有阻礙性，不得防止用戶行使其權利，例如：透過收取額外費用。

<u>How to help users in securing the storage of their personal data in their own systems?</u>

<u>如何協助用戶確保在其自身系統中所儲存個人資料之安全性？</u>

By retrieving their personal data from an online service, there is always the risk that users may store them in less secured systems than the one provided by the service. The data subject requesting the data is responsible for identifying the right measures in order to secure personal data in his own system. However, he should be made aware of this in order to take steps to protect the information he has received. As an example of leading practice data controllers may also recommend appropriate format(s), encryption tools and other security measures to help the data subject in achieving this goal.

透過網路服務取得個人資料，用戶難免有可能將其資料儲存於比較不安全（相較於服務所

[37] In conformance to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
符合第2016/1148號指令（EU）關於整體歐盟網路和資訊系統高度共同安全保護措施。

提供之系統）的系統中之風險。請求資料之當事人為了確保個人資料於其自身之系統中之安全，有責任識別正確之措施。然而，該當事人必須能瞭解到此情況，以便採取措施保護接收之資訊。作為主要實務示例，資料控管者亦可推薦適當之格式、加密工具和其他安全措施，以協助當事人實現此目標。

* * *

Done in Brussels, on 13 December 2016
2016年12月13日於布魯塞爾完成

For the Working Party,
工作小組
The Chairwoman
主席
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017
2017年4月5日最後修訂並通過
For the Working Party
工作小組
The Chairwoman
主席
Isabelle FALQUE- PIERROTIN

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN
WP 244 rev.01

Guidelines for identifying a controller or processor's lead supervisory authority

關於識別控管者或受託運用者的主責監管機關之指引

Adopted on 13 December 2016

2016年12月13日通過

As last Revised and Adopted on 5 April 2017

2017年4月5日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35
由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm
網址：http://ec.europa.eu/justice/data-protection/index_en.htm

Table of Content
目錄

1. Identifying a lead supervisory authority: the key concepts
識別主責監管機關：關鍵概念

1.1 'Cross-border processing* of personal data'
「個人資料之跨境運用」

Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data. Article 4(23) of the General Data Protection Regulation (GDPR) defines 'cross-border processing' as either the:
識別主責監管機關僅在控管者或受託運用者執行個人資料之跨境運用時始相關聯。「一般資料保護規則」（GDPR）第4條第23款將「跨境運用」定義為：

- *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or the*
  當控管者或受託運用者設置於一個以上成員國境內，而個人資料之運用發生於控管者或受託運用者位於歐盟境內一個以上成員國據點之活動範圍內;抑或

- *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*
  個人資料之運用發生於控管者或受託運用者位於歐盟境內之單一據點之活動範圍內，然該運用實質影響或可能實質影響位於一個以上成員國境內之當事人。

This means that where an organisation has establishments in France and Romania, for example, and the processing of personal data takes place in the context of their activities, then this will constitute cross-border processing.
此意味著，例如，若一個組織在法國和羅馬尼亞設有據點，且個人資料之運用是發生於該據點之活動範圍內，則將構成跨境運用。

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Alternatively, the organisation may only carry out processing activity in the context of its establishment in France. However, if the activity substantially affects – or is likely to substantially affect - data subjects in France and Romania then this will also constitute cross-border processing.
抑或，該組織僅在其位於法國據點的活動範圍內進行運用。然而，若該活動實質影響或可能實質影響 － 位於法國和羅馬尼亞之當事人，則亦將構成跨境運用。

1.1.1 'Substantially affects'
「實質性影響」

The GDPR does not define 'substantially' or 'affects'. The intention of the wording was to ensure that not all processing activity, with any effect and that takes place within the context of a single establishment, falls within the definition of 'cross-border processing'.
GDPR並未就「實質性」或「影響」加以定義。此措辭之目的係為確保並非任何有影響且發生於某單一據點範圍內之所有運用活動皆落入「跨境運用」之定義。

The most relevant ordinary English meanings of 'substantial' include; 'of ample or considerable amount or size; sizeable, fairly large', or 'having solid worth or value, of real significance; solid; weighty, important' (Oxford English Dictionary).
與「實質性」最相關之一般英語含義包括：「足夠或相當之數量或大小；相當多的、相當大的」或「具有實質之價值或重要性；具有重要意義；實在的；重大的、重要的」（牛津英語詞典）。

The most relevant meaning of the verb 'affect' is 'to influence' or 'to make a material impression on'. The related noun -'effect'- means, amongst other things, 'a result' or 'a consequence' (Oxford English Dictionary). This suggests that for data processing to *affect* someone it must have some form of impact on them. Processing that does not have a substantial effect on individuals does not fall within the second part of the definition of 'cross-border processing'. However, it would fall within the first part of the definition where the processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union, where the controller or processor is established in more than one Member State.
與「影響」此動詞最相關之含義為「影響力」或「留下深刻印象」。相關名詞 － 「影響」 － 之含義很多，其一為「結果」或「後果」（牛津英語詞典）。此意味者，對於*影響*某人之資料運用，該運用必須對該人產生某種形式之影響。對個人沒有實質性影響之運用不符合「跨境運用」定義中之第二部分。然而，當控管者或受託運用者設置於一個以上成員國境內，而個人資料之運用發生於控管者或受託運用者位於歐盟境內一個以

上成員國據點之活動範圍內，則該運用將符合定義的第一部分。

Processing can be brought within the second part of the definition if there is the likelihood of a substantial effect, not just an actual substantial effect. Note that 'likely to' does not mean that there is a remote possibility of a substantial effect. The substantial effect must be more likely than not. On the other hand, it also means that individuals do not have to be actually affected: the likelihood of a substantial effect is sufficient to bring the processing within the definition of 'cross-border processing'.
只要存在實質性影響之可能性，而非實際上有實質性影響，運用即可屬於該定義中之第二部分。須注意者為，「可能」並非意味著存在實質性影響之微小可能性。實質性影響必須更接近可能。另一方面，此也意味著個人不須實際上受到影響：只要有實質性影響之可能性即足以使運用屬於「跨境運用」之定義範圍內。

The fact that a data processing operation may involve the processing of a number – even a large number – of individuals' personal data, in a number of Member States, does not necessarily mean that the processing has, or is likely to have, a substantial effect. Processing that does not have a substantial effect does not constitute cross-border processing for the purposes of the second part of the definition, regardless of how many individuals it affects.
資料運用作業可能涉及在數個成員國中運用多個 – 甚至是大量 – 當事人個人資料之事實並不一定意味著運用具有或可能具有實質性之影響。就定義之第二部分而言，沒有實質性影響之運用即不構成跨境運用，無論有多少個人受其影響。

Supervisory Authorities will interpret 'substantially affects' on a case by case basis. We will take into account the context of the processing, the type of data, the purpose of the processing and factors such as whether the processing:
監管機關將依據具體個案情況解釋「實質性影響」。我們將考量運用之背景、資料之類型、運用之目的以及下列因素，例如運用是否：

- causes, or is likely to cause, damage, loss or distress to individuals;
  造成或可能造成對當事人之損害、損失或痛苦；
- has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity;
  在限制權利或拒絕機會上具有或可能具有實際影響；
- affects, or is likely to affect individuals' health, well-being or peace of mind;
  影響或可能影響個人之健康、福祉或平靜；

- affects, or is likely to affect, individuals' financial or economic status or circumstances;
  影響或可能影響個人之財務或經濟狀態或情況；
- leaves individuals open to discrimination or unfair treatment;
  使個人受到歧視或不公平待遇；
- involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children;
  涉及分析特殊類型之當事人資料或其他侵入性資料，尤其是兒童之個人資料；
- causes, or is likely to cause individuals to change their behaviour in a significant way;
  造成或可能造成個人以顯著之方式改變其行為；
- has unlikely, unanticipated or unwanted consequences for individuals;
  對個人產生不可能、未預期或不希望之後果；
- creates embarrassment or other negative outcomes, including reputational damage; or
  造成困窘或其他負面之結果，包括名譽受損；或
- involves the processing of a wide range of personal data.
  涉及運用廣泛之個人資料。

Ultimately, the test of 'substantial effect' is intended to ensure that supervisory authorities are only required to co-operate formally through the GDPR's consistency mechanism *"where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States". (Recital 135)*
最終，對「實質性影響」之檢驗旨在*「當某監管機關有意就實質上影響數個成員國境內大量當事人之運用作業採取產生法律效果之措施時」（前言第135點）*，確保各監管機關透過GDPR一致性機制進行正式合作。

1.2 Lead supervisory authority.
主責監管機關

Put simply, a 'lead supervisory authority' is the authority with the primary responsibility for

dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data.
簡而言之，「主責監管機關」是主要負責處理跨境資料運用活動之機關，例如若當事人對其個人資料之運用提出申訴時。

The lead supervisory authority will coordinate any investigation, involving other 'concerned' supervisory authorities.
主責監管機關將協調任何涉及其他「有關」監管機關之調查。

Identifying the lead supervisory authority depends on determining the location of the controller's 'main establishment' or 'single establishment' in the EU. Article 56 of the GDPR says that:
識別主責監管機關取決於確認控管者位於歐盟境內「主要據點」或「單一據點」之位置。GDPR第56條規定：

- *the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the* [cooperation] *procedure provided in Article 60.*
  控管者或受託運用者之主要據點或單一據點的監管機關，為了第60條規定之（合作）程序，應足擔任該控管者或受託運用者之跨境運用行為的主責監管機關。

1.3 Main establishment.
主要據點

Article 4(16) of the GDPR states that 'main establishment' means:
GDPR第4條第16款規定「主要據點」係指：

- *as regards a controller with establishments in more than one Member State, the place of its* ***central administration*** *in the Union, unless the* ***decisions on the purposes and means*** *of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the* ***power to have such decisions implemented****, in which case the establishment having taken such decisions is to be considered to be the main establishment;*
  *就於一個以上成員國設有據點之控管者而言，其位於歐盟境內之**中央管理機構**所在地，除非關於個人資料**運用之目的和方式**係由控管者位於歐盟的另一個據點所**決定**，且該後者據點**有權執行此決定**，於此種情況下，作出決定之據點應被視為主要據點；*

- *as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;*

  就於一個以上成員國設有據點之受託運用者而言，其位於歐盟境內之中央管理機構所在地，抑或，若受託運用者在歐盟境內並無中央管理機構時，則以受託運用者在歐盟境內主要運用活動發生之據點，且於該據點之活動範圍內受託運用者受本規則規定之特定義務所拘束。

2. Steps to identify the lead supervisory authority
識別主責監管機關之步驟

2.1 Identify the 'main establishment' for controllers
識別控管者之「主要據點」

In order to establish where the main establishment is, it is firstly necessary to identify the central administration of the data controller in the EU, if any.[1] The approach implied in the GDPR is that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented.

為了確認主要據點之位置，首先必須識別資料控管者位於歐盟境內之中央管理機構(若有)。[1] GDPR之識別方法為，位於歐盟的中央管理機構係就運用個人資料之目的和方式作出決策之所在地，且該所在地有權力執行此決策。

The essence of the lead authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU. In cases where decisions relating to different cross-border processing activities are taken within the EU central administration, there will be a single lead supervisory authority for the various data processing activities carried out by the multinational company. However, there may be cases where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity. This means that there can be situations where more than one lead authority can be identified, i.e. in cases

[1] The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement. The GDPR is currently under scrutiny for incorporation, see http://www.efta.int/eea-lex/32016R0679
GDPR與歐洲經濟區相關聯，並將在納入歐洲經濟區協議後適用。GDPR目前正在就此議題接受審查，請參閱http://www.efta.int/eea-lex/32016R0679

where a multinational company decides to have separate decision making centres, in different countries, for different processing activities.
GDPR的主責機關原則其本質在於跨境運用之監督應由歐盟內之單一監管機關領導。若由位於歐盟境內之中央管理機構執行各種跨境運用活動相關之決策，則該跨國公司執行的各種資料運用活動將只有一個單一主責監管機關。然而，由中央管理機構以外之據點就特定運用活動之目的和方式做出自主決策之情況亦可能存在。此意味著當跨國公司決定在不同國家就不同運用活動設置個別決策中心時，可能會有得識別多個主責機關之情形。

It is worth recalling, that where a multinational company centralises all the decisions relating to the purposes and means of processing activities in one of its establishments in the EU (and that establishment has the power to implement such decisions), only one lead supervisory authority will be identified for the multinational.
值得再次提醒者為，若一家跨國公司將和運用活動目的及方式相關之所有決策集中於位於歐盟境內的某一據點處理時(且該據點有權力執行此類決策)，則就該跨國公司而言，只會被有一個主責監管機關需認定。

In these situations it will be essential for companies to identify precisely where the decisions on purpose and means of processing are taken. Correct identification of the main establishment is in the interests of controllers and processors because it provides clarity in terms of which supervisory authority they have to deal with in respect of their various compliance duties under the GDPR. These may include, where relevant, designating a data protection officer or consulting for a risky processing activity that the controller cannot mitigate by reasonable means. The relevant provisions of the GDPR are intended to make these compliance tasks manageable.
於這些情況下，公司必須準確識別制訂與運用目的和方式相關決策之所在地。正確識別符合控管者和受託運用者之利益之主要據點，因為如此可使其釐清為符合GDPR下各種合規性義務時所應交涉之監管機關。這些相關情形可能包括指定個資保護長或當控管者無法透過合理方式減輕運用活動風險時之諮詢。GDPR相關規定旨在使這些合規性任務易於管理。

The examples below illustrate this:
以下示例說明此一概念：

Example 1: A food retailer has its headquarters (i.e. its 'place of central administration') in Rotterdam, Netherlands. It has establishments in various other EU countries, which are in contact with individuals there. All establishments make use of the same software to process consumers' personal data for marketing purposes. All the decisions about the purposes and means of the processing of consumers' personal data for marketing purposes are taken within its Rotterdam headquarters. This means that the company's lead supervisory authority for this cross border processing activity is the Netherlands supervisory authority.

示例1：一食品零售商總部（即其「中央管理機構」）設置於荷蘭鹿特丹。該公司在歐盟其他國家設有據點，且由這些據點與在地當事人聯繫。基於行銷目的，所有據點皆使用相同軟體以運用消費者之個人資料。關於為行銷目的運用消費者個人資料之目的和方式的所有決策皆由鹿特丹總部執行。此意味著該公司跨境運用活動的主責監管機關係荷蘭監管機關。

Example 2: A bank has its corporate headquarters in Frankfurt, and all[2] its banking processing activities are organised from there, but its insurance department is located in Vienna. If the establishment in Vienna has the power to decide on all insurance data processing activity and to implement these decisions for the whole EU, then as foreseen in Art 4(16) of the GDPR, the Austrian supervisory authority would be the lead authority in respect of the cross border processing of personal data for insurance purposes, and the German authorities (Hessen supervisory authority) would supervise the processing of personal data for banking purposes, wherever the clients are located. [3]

示例2:一銀行的企業總部設置於法蘭克福,且所有[2]銀行運用活動皆由該總部組織策劃，但其保險部門設置於維也納。若位於維也納之據點有權決定整體歐盟所有保險資料之運用活動並執行這些決策，則正如GDPR第4條第1款所預見，奧地利監管機關將是為保險目的所為之跨境個人資料運用的主責監管機關。而德國當局（黑森州監管機關）將監督以銀行業務目的所為之個人資料運用，無論其客戶所在位置為何。[3]

[2] In the context of processing personal data for banking purposes, we recognise that are many different processing activities involved in this. However, to simplify matters, we address all of them as a single purpose. The same is true of processing done for insurance purposes.
在為銀行目的運用個人資料之背景下，我們認識到此情形涉及許多不同之運用活動。然而，為了簡化問題，我們將這些運用皆視作單一目的。同樣之概念亦適用於為保險目的而進行之運用。

[3] It should be recalled also that the GDPR provides for the possibility of local oversight in specific cases. See Recital (127): *"Each supervisory authority* ***not acting as the lead*** *supervisory authority* ***should be competent to handle local cases*** *where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns* ***only processing carried out in a single Member State and involves only data subjects in that single Member State****, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State."* This principle means that the supervision of HR data connected to local employment context could fall to several supervisory authorities.
另應記住，GDPR提供了在特定情況下進行當地監管之可能性。請參閱前言第127點：「*每個****不做為主責監管機關之監管機關應有權處理****設置於一個以上成員國之控管者或受託運用者的****當地案件****，當具體運用*

2.1.1 Criteria for identifying a controller's main establishment in cases where it is not the place of its central administration in the EU

當歐盟並非中央管理機構之所在地時，識別控管者主要據點之標準

Recital 36 of the GDPR is useful in clarifying the main factor that shall be used to determine a controller's main establishment if the criterion of the central administration does not apply. This involves identifying where the effective and real exercise of management activities, that determine the main decisions as to the purposes and means of processing through stable arrangements, takes place. Recital 36 also clarifies that "the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment".

若中央管理機構之標準不適用，GDPR前言第36點有助於闡明決定控管者主要據點之主要因素。此涉及識別管理活動的有效和實際發生地，透過穩定安排，這些管理活動就運用之目的和方式做出了主要決策。前言第36點亦闡明「為運用個人資料或運用活動所存在或使用之技術方法和科技本身並不構成主要據點，因此不得作為決定主要據點之標準」。

The data controller itself identifies where its main establishment is and therefore which supervisory authority is its lead authority. However, this can be challenged by the respective supervisory authority concerned afterwards.

資料控管者自行識別其主要據點之所在地，進而識別何監管機關為其主責機關。然而，此決定在日後可能受到個別有關監管機關之挑戰。

The factors below are useful for determining the location of a controller's main establishment, according to the terms of the GDPR, in cases where it is not the location of its central administration in the EU.

依據GDPR之條款，若歐盟並非中央管理機構之所在地時，以下因素可協助決定控管者主要據點之所在地。

- Where are decisions about the purposes and means of the processing given final 'sign off'?
  關於運用目的和方式之決策，最終「許可」所在地為何？
- Where are decisions about business activities that involve data processing made?

---

*之主題內容**僅涉及在單一成員國境內進行之運用和僅涉及該單一成員國境內之當事人**，例如，當主題內容涉及在某一成員國之特定僱傭運用員工之個人資料時。*」此原則意味著對與當地僱傭環境相關人力資源資料之監督，可能隸屬於數個監管機關。

關於涉及資料運用之商業活動之決策所在地為何？

- Where does the power to have decisions implemented effectively lie?
  有效執行決策之權力所在地為何？
- Where is the Director (or Directors) with overall management responsibility for the cross border processing located?
  對跨境運用負有全面管理責任之董事（或董事們）所在地為何？
- Where is the controller or processor registered as a company, if in a single territory?
  若在單一領土內，控管者或受託運用者所註冊之公司所在地為何？

Note that this is not an exhaustive list. Other factors may be relevant depending on the controller or processing activity in question. If a supervisory authority has reasons to doubt that the establishment identified by the controller is in reality the main establishment for the purposes of the GDPR, it can – of course – require the controller to provide the additional information necessary for it to prove where its main establishment is located.
需注意此並非詳盡列舉之清單，還有其他因素亦可能相關，端視所涉及之控管者或運用活動而決定。若監管機關有理由懷疑控管者所識別之據點實際上是否為GDPR之主要據點，監管機關當然可要求控管者提供必要之額外資訊，以證明其主要據點之所在地。

2.1.2 Groups of undertakings
企業集團

Where processing is carried out by a group of undertakings that has its headquarters in the EU, the establishment of the undertaking with overall control is presumed to be the decision-making centre relating to the processing of personal data, and will therefore be considered to be the main establishment for the group, except where decisions about the purposes and means of processing are taken by another establishment. The parent, or operational headquarters of the group of undertakings in the EU, is likely to be the main establishment, because that would be the place of its central administration.
若運用係由總部設立於歐盟境內之企業集團所為，且該控制整體企業之據點被認為是與個人資料運用相關之決策中心，則該據點將因此被視為係該集團之主要據點，除非與運用目的和方式相關之決策係由另一據點為之。位於歐盟境內企業集團之母公司或營運總部很有可能是主要據點，因其可能是中央管理機構之所在地。

The reference in the definition to the place of a controller's central administration works well for organisations that have a centralised decision-making headquarters and branch-type

structure. In such cases it is clear that the power to make decisions about cross-border data processing, and to have them carried out, lies within the company's headquarters. In such cases, determining the location of the main establishment – and therefore which supervisory authority is the lead supervisory authority - is straightforward. However, the decision system of group of companies could be more complex, giving independent making powers relating to cross border processing to different establishments. The criteria set out above should help groups of undertakings to identify their main establishment.

控管者中央管理機構所在地之定義的參考標準，對擁有集中式決策總部和分支機構結構的組織也很適用。於此種情況下，作出跨境資料運用決策並執行這些決策之權力很明顯地屬於企業總部。於此種情況下，確認主要據點之所在地 – 以及何監管機關因而成為主責監管機關 – 應為明確。然而，企業集團會賦予不同據點有關跨境運用之獨立決策權，因此決策系統可能更加複雜。上述標準應有助於企業集團識別其主要據點。

2.1.3 Joint data controllers
共同資料控管者

The GDPR does not specifically deal with the issue of designating a lead authority where two or more controllers established in the EU jointly determine the purposes and means of processing – i.e. joint controllers. Article 26(1) and Recital 79 make it clear that in joint controller situations, the controllers shall in a transparent manner determine their respective responsibilities for compliance with their obligations under the Regulation. In order, therefore, to benefit from the one-stop-shop principle, the joint controllers should designate (among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out in the joint controller situation. The arrangement of the joint controllers is without prejudice to the liability rules provided in the GDPR, in particular in Article 82(4).

當兩個或多個設立於歐盟境內之控管者共同決定運用目的和方式 – 即共同控管者時，GDPR並未特別就指定主責機關之議題進行處理。第26條第1項和前言第79點明確規定，於共同控管者之情況下，控管者應以透明之方式確認各自履行本規則義務之責任。因此，為了從一站式原則中受益，共同控管者應（從各決策據點中）指定何共同控管者之據點將有權執行所有共同控管者關於運用之決策。而該據點將被視為在共同控管者之情形下進行運用之主要據點。共同控管者之安排並不影響GDPR所規範之賠償責任，尤其是第82條第4項。

2.2 Borderline cases

爭議案件

There will be borderline and complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken. This might be the case where there is cross-border processing activity and the controller is established in several Member States, but there is no central administration in the EU and none of the EU establishments are taking decisions about the processing (i.e. decisions are taken exclusively outside of the EU).

也會有一些難以識別主要據點或確認關於資料運用之決策係於何處進行等具爭議性和複雜之情況出現。可能之情況為跨境運用活動，且控管者設立於數個成員國境內，但於歐盟並無中央管理機構，且位於歐盟之據點亦未就運用做出決策（即決策完全於歐盟境外為之）。

In the case above, the company carrying out cross border processing may be keen to be regulated by a lead authority to benefit from the one-stop-shop principle. However, the GDPR does not provide a solution for situations like this. In these circumstances, the company should designate the establishment that has the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets, as its main establishment. If the company does not designate a main establishment in this way, it will not be possible to designate a lead authority. Supervisory authorities will always be able to investigate further where this is appropriate.

在上述情況下，實施跨境運用之公司可能希望受到單一主責機關之監管，以便受益於一站式原則。然而，GDPR並未就此種情況提供解決方案。於此種情狀下，該公司應指定某一據點作為其主要據點，而該據點有權執行關於運用活動之決策，並對運用承擔責任，包括擁有足夠之資產，作為主要據點。若公司並未以此種方式指定主要據點，則無法指定主責機關。各監管機關將始終得酌情進一步調查。

The GDPR does not permit ‘forum shopping’. If a company claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision making over the processing of personal data takes place there, the relevant supervisory authorities (or ultimately EDPB) will decide which supervisory authority is the ‘lead’, using objective criteria and looking at the evidence. The process of determining where the main establishment is may require active inquiry and co-operation by the supervisory authorities. Conclusions cannot be based solely on statements by the organisation under review. The burden of proof ultimately falls on controllers and processors to demonstrate to the relevant supervisory authorities where the relevant processing decisions are taken and

where there is the power to implement such decisions. Effective records of data processing activity would help both organisations and supervisory authorities to determine the lead authority. The lead supervisory authority, or concerned authorities, can rebut the controller's analysis based on an objective examination of the relevant facts, requesting further information where required.

GDPR不允許「挑選主責機關」。若某公司聲稱其主要據點設置於某一個成員國境內，但於該據點並無採取有效和實際之管理活動或個人資料運用之決策，相關監管機關（或最終EDPB）將使用客觀標準並查看證據以決定何監管機關為「主責機關」。確認主要據點所在地之程序可能需要監管機關的積極調查與合作。所得結論不得僅基於受審查組織之陳述。控管者和受託運用者負有最終舉證責任，以向有關監管機關證明相關運用決策之發生地以及有權執行這些決策之所在地。有效之資料運用活動記錄將有助於組織和監管機關確認主責機關。主責監管機關或有關機關可依據對相關事實的客觀審查以駁回控管者之分析，並在必要時要求提供進一步資訊。

In some cases the relevant supervisory authorities will ask the controller to provide clear evidence, in line with any EDPB guidelines, of where its main establishment is, or where decisions about a particular data processing activity are taken. This evidence will be given due weight and the supervisory authorities involved will co-operate to decide which one of them will take the lead in investigations. Such cases will only be referred to the EDPB for a decision under Article 65(1)(b) where supervisory authorities have conflicting views in terms of identifying the lead supervisory authority. However, in most cases, we expect that the relevant supervisory authorities will be able to agree a mutually satisfactory course of action.

在某些情況下，相關監管機關將要求控管者依據EDPB指引提供其主要據點所在地或於何地做出某特定資料運用活動決策之明確證據。這些證據將被給予應有之重視，且相關監管機關將合作決定何機關將主導調查。此類案件僅有當監管機關在識別主責監管機關方面存在相互矛盾之觀點時，始得依據第65條第1項第b款之規定提交EDPB作出決定。然而，在大多數情況下，我們期待相關監管機關能夠達成一個相互滿意的行動方針。

2.3 Processor
受託運用者

The GDPR also offers the one-stop-shop system for the benefit of data processors that are subject to GDPR and have establishments in more than one Member State.

當該受託運用者於一個以上之成員國設置據點時，GDPR亦為受其規範之受託運用者之利益提供一站式系統。

Article 4(16)(b) of the GDPR states that the processor's main establishment will be the place

of the central administration of the processor in the EU or, if there is no central administration in the EU, the establishment in the EU where the main processing (processor) activities take place.

GDPR第4條第16款第b目規定，受託運用者之主要據點將是其位於歐盟境內之中央管理機構所在地，或若於歐盟並無中央管理機構，則是其位於歐盟之據點，且該據點為主要運用（受託運用者）活動發生之所在地。

However, according to Recital 36, in cases involving both controller and processor, the competent lead supervisory authority should be the lead supervisory authority for the controller. In this situation, the supervisory authority of the processor will be a 'supervisory authority concerned' and should participate in the cooperation procedure. This rule will only apply where the controller is established in the EU. In cases when controllers are subject to the GDPR on the basis of Art 3(2), they will not be subject to the one-stop-shop mechanism. A processor may provide services to multiple controllers located in different Member States – for example, a large cloud-service provider. In such cases, the lead supervisory authority will be the supervisory authority that is competent to act as lead for the controller. In effect, this means a processor may have to deal with multiple supervisory authorities.

然而，依據前言第36點，在同時涉及控管者和受託運用者之情況下，權責主責監管機關應係控管者之主責監管機關。在此情況下，受託運用者之監管機關將是「有關監管機關」，且應參與合作程序。此規則僅適用於當控管者設置於歐盟境內之情況。若控管者係基於第3條第2項而受GDPR所拘束，則將不適用一站式機制。受託運用者可能向位於不同成員國之多個控管者提供服務 － 例如，大型雲端服務提供商。於此種情況下，主責監管機關將是有能力主導控管者之監管機關。實際上，此意味著受託運用者可能必須與多個監管機關交涉。

3. Other relevant issues
其他相關問題

3.1 The role of the 'supervisory authority concerned'
「有關監管機關」之角色

GDPR Article 4(22) says that the:

GDPR第4條第22款規定：

> *'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory*

authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority.

「有關監管機關」係指與個人資料運用相關之監管機關，因：（a）控管者或受託運用者設置於該監管機關所在成員國之領土上；（b）居住於該監管機關所在成員國之當事人被該運用所實質影響或可能實質影響；或（c）已向該監管機關提出申訴。

The concept of a concerned supervisory authority is meant to ensure that the 'lead authority' model does not prevent other supervisory authorities having a say in how a matter is dealt with when, for example, individuals residing outside the lead authority's jurisdiction are substantially affected by a data processing activity. In terms of factor (a) above, the same considerations as for identifying a lead authority apply. Note that in (b) the data subject must merely reside in the Member State in question; he or she does not have to be a citizen of that state. It will generally be easy – in (c) to determine – as a matter of fact – whether a particular supervisory authority has received a complaint.

有關監管機關之概念旨在確保「主責機關」模式不會妨礙其他監管機關針對問題處理有表達意見的權利，例如，當資料運用活動實質影響到居住於主責機關管轄範圍以外之當事人時。就上述要素（a）而言，適用於與識別主責機關相同之考量要件。另應注意，在要素（b）中，當事人僅須位於相關成員國境內；而不須係該國家之公民。在要素（c）中確認某特定監管機關是否收到申訴之事實通常是很容易的。

Article 56, paragraphs (2) and (5) of the GDPR provide for a concerned supervisory authority to take a role in dealing with a case without being the lead supervisory authority. When a lead supervisory authority decides not to handle a case, the concerned supervisory authority that informed the lead shall handle it. This is in accordance with the procedures in Article 61 (Mutual assistance) and Article 62 (Joint operations of supervisory authorities) of the GDPR. This might be the case where a marketing company with its main establishment in Paris launches a product that only affects data subjects residing in Portugal. In such a case the French and Portuguese supervisory authorities might agree that it is appropriate for the Portuguese supervisory authority to take the lead in dealing with the matter. Supervisory authorities may request that data controllers provide input in terms of clarifying their corporate arrangements. Given that the processing activity has a purely local effect – i.e. on individuals in Portugal – the French and Portuguese supervisory authorities have the discretion to decide which supervisory authority should deal with the matter – in accordance

with Recital 127.
GDPR第56條第2項和第5項提供了有關監管機關在不作為主責監管機關之情況下處理案件時應扮演之角色。當主責監管機關決定不處理某案件時，先前通知主責機關之該有關監管機關應當予以處理。如此符合GDPR第61條（相互協助）和第62條（監管機關聯合作業）所規定之程序。可能之情況為，一間行銷公司在其位於巴黎之主要據點推出的產品僅影響居住於葡萄牙之當事人。於此情況下，法國和葡萄牙之監管機關可能會同意由葡萄牙監管機關就此事為主責機關較為合適。監管機關可要求資料控管者在澄清其公司安排方面提供意見。鑑於運用活動具有完全之地方性效果 – 即對葡萄牙之個人 – 法國和葡萄牙監管機關有權依據前言第127點決定由何監管機關處理此案件。

The GDPR requires lead and concerned supervisory authorities to co-operate, with due respect for each other's views, to ensure a matter is investigated and resolved to each authority's satisfaction – and with an effective remedy for data subjects. Supervisory authorities should endeavour to reach a mutually acceptable course of action. The formal consistency mechanism should only be invoked where co-operation does not reach a mutually acceptable outcome.
GDPR要求主責和有關監管機關於適當尊重彼此意見之情況下進行合作，以確保每個機關就案件之調查和結果皆為滿意，並為當事人提供有效之補償措施。監管機關應致力達成相互可接受之行動方案。只有在合作未能達到相互可接受結果之情況下，始得援引正式之一致性機制。

The mutual acceptance of decisions can apply to substantive conclusions, but also to the course of action decided upon, including enforcement activity (e.g. full investigation or an investigation with limited scope). It can also apply to a decision not to handle a case in accordance with GDPR, for example because of a formal policy of prioritisation, or because there are other concerned authorities as described above.
相互可接受之決定可適用於實質性之結論，但亦適用於決策之行動方案，包括執法活動（例如全面調查或有限範圍之調查）。其亦可適用於依據GDPR不處理案件之決定，例如因正式之優先權政策，或因存在如上所述之其他有關機關。

The development of consensus and good will between supervisory authorities is essential to the success of the GDPR's cooperation and consistency process.
監管機關之間建立共識和善意對於達成GDPR之合作和一致性程序至關重要。

3.2 Local processing.
在地運用

Local data processing activity does not fall within the GDPR's cooperation and consistency provisions. Supervisory authorities will respect each other's competence to deal with local data processing activity on a local basis. Processing carried out by public authorities will always be dealt with on a 'local' basis too.

在地資料運用活動不屬於GDPR合作和一致性之規定範圍。監管機關將尊重彼此於當地處理在地資料運用活動之能力。公務機關所進行之運用也始終係於「在地」之基礎上處理之。

3.3 Companies not established within the EU.
非設置於歐盟境內之公司

The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a Member State does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative.

GDPR之合作和一致性機制僅適用於在歐盟境內設有一個或多個據點之控管者。若公司在歐盟境內沒有據點，僅於某一成員國設置代表並不會觸發一站式系統。此意味著並未於歐盟設置任何據點之控管者必須透過當地代表與位於其活動發生地每個成員國之當地監管機關進行交涉。

Done in Brussels, on 13 December 2016

2016年12月13日於布魯塞爾完成

For the Working Party,

工作小組

The Chairwoman

主席

Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

2017年4月5日最後修訂並通過

For the Working Party

工作小組

The Chairwoman

主席

Isabelle FALQUE-PIERROTIN

ANNEX - Questions to guide the identification of the lead supervisory authority
附錄 － 指導識別主責監管機關之提問

1. Is the controller or processor carrying out the cross-border processing of personal data?
控管者或受託運用者是否進行跨境個人資料運用？

a. Yes, if:
是，若:

- the controller or processor is established in more than one Member State and
控管者或受託運用者設置於一個以上成員國境內，且
- the processing of personal data takes place in the context of the activities of establishments in more than one Member State.
個人資料之運用在一個以上成員國之據點之活動範圍內發生。

➢ In this case, go to section 2.
於此種情況下，請參閱第2項。

b. Yes, if:
是，若:

- the processing of personal data takes place in the context of the activities of a data controller or processor's single establishment in the Union, but:
個人資料之運用是在資料控管者或受託運用者位於歐盟境內之單一據點之活動範圍內發生，但：
- substantially affects or is likely to substantially affect individuals in more than one Member State.
實質影響或可能實質影響一個以上成員國境內之當事人。

➢ In this case, the lead authority is the authority for the controller or processor's single establishment in a single Member State. This must – by logic - be the controller or processor's main establishment because it is its only establishment.
於此種情況下，主責機關係控管者或受託運用者位於某單一成員國境內單一據點之機關。該據點必須 － 邏輯上 － 係控管者或受託運用者之主

要據點，因其是唯一之據點。

2. How to identify the 'lead supervisory authority'
如何識別「主責監管機關」

a. In a case involving only a controller:
於僅涉及控管者之情況下：

i. Identify the controller's place of central administration in the EU;
識別控管者位於歐盟境內之中央管理機構所在地；

ii. The supervisory authority of the country where the place of central administration is located is the controller's lead authority.
中央管理機構所在國家之監管機關係控管者之主責機關。

However:
然而：

iii. If decisions on the purposes and means of the processing are taken in another establishment in the EU, and that establishment has the power to implement those decisions, then the lead authority is the one located in the country where this establishment is.
若關於運用目的和方式之決策係由位於歐盟之另一個據點所進行，且該據點有權執行這些決策時，主責機關為位於該據點所在國家之監管機關。

b. In a case involving a controller and a processor:
於涉及控管者和受託運用者之情況下：

i. Check if the controller is established in the EU and subject to the one-stop-shop system. If so,
確認控管者是否設置於歐盟境內，並受一站式系統所拘束。如是，

ii. Identify the lead supervisory authority of the controller. This authority will also be the lead supervisory authority for the processor.
識別控管者之主責監管機關。該機關亦為受託運用者之主責監管機關。

iii. The (non-lead) supervisory authority competent for the processor will be a 'concerned authority' – see 3 below.
受託運用者之（非主責）權責監管機關將屬於「有關機關」－ 請參閱下

文第3項。

c. In a case involving only a processor:
於僅涉及受託運用者之情況下：

i. Identify the processor's place of central administration in the EU;
識別受託運用者位於歐盟境內之中央管理機構所在地；

ii. If the processor has no central administration in the EU, identify the establishment in the EU where the main processing activities of the processor take place.
若受託運用者在歐盟並無中央管理機構，則識別受託運用者於歐盟主要運用活動發生之據點。

d. In a case involving joint controllers:
於涉及共同控管者之情況下：

i. Check if the joint controllers are established in the EU.
確認共同控管者是否設置於歐盟境內。

ii. Designate among the establishments where decisions on the purposes and means of the processing are taken the establishment which has the power to implement these decisions with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out by the joint controllers. The lead authority is the one located in the country where this establishment is.
於各據點間指定就運用目的和方式進行決策之據點，且該據點有權對所有共同控管者執行這些決策。該據點因而將被視為共同控管者進行運用之主要據點。主責機關即為該據點所在國家之監管機關。

3. Are there any 'concerned supervisory authorities'?
是否存在「有關監管機關」?

An authority is a 'concerned authority':
某機關屬於「有關機關」：

- when the controller or processor has an establishment on its territory, or:
當控管者或受託運用者於其境內設置據點時，或
- when data subjects on its territory are substantially affected or likely to be

substantially affected by the processing, or:
當運用實質影響或可能實質影響於其境內之當事人時，或

- when a complaint is received by a particular authority.
  當特定機關收到申訴案件。

ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

17/EN

WP 253

Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

關於第2016/679號規則(GDPR)中的行政罰鍰適用和制定之指引

Adopted on 3 October 2017

2017年10月3日通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立。為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 03/075號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日之第95/46/EC號指令而設立，

基於該指令第29條及第30條，

基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Table of contents 目錄

I. Introduction
導言

The EU has completed a comprehensive reform of data protection regulation in Europe. The reform rests on several pillars (key components): coherent rules, simplified procedures, coordinated actions, user involvement, more effective information and stronger enforcement powers.
歐盟已完成歐洲資料保護規則的全面性改革。此改革係基於幾項支柱（關鍵構成要素）：一致性之規則、簡化之程序、協調之行動、使用者之參與、更有效之資訊及更強大之執法權力。

Data controllers and data processors have increased responsibilities to ensure that personal data of the individuals is protected effectively. Supervisory authorities have powers to ensure that the principles of the General Data Protection Regulation (hereafter 'the Regulation') as well as the rights of the individuals concerned are upheld according to the wording and the spirit of the Regulation.
資料控管者和資料受託運用者被附加了更多的責任，以確保有效保護當事人之個人資料。監管機關有權確保一般資料保護規則（以下簡稱「本規則」）之原則及相關之個人權利，已依據本規則之文義和精神予以維護。

Consistent enforcement of the data protection rules is central to a harmonized data protection regime. Administrative fines are a central element in the new enforcement regime introduced by the Regulation, being a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures provided by article 58.
資料保護規則的一致性執法是調和資料保護制度之核心。行政罰鍰係本規則所引進新執法制度之核心要素，另加上第58條規定之其他措施，構成監管機關有力之執法工具。

This document is intended for use by the supervisory authorities to ensure better application and enforcement of the Regulation and expresses their common understanding of the provisions of article 83 of the Regulation as well as its interplay with articles 58 and 70 and their corresponding recitals.
本文件旨在提供監管機關使用，以確保更好地適用和執行本規則，並表達監管機關對本規則第83條規定之共識，以及與第58條、第70條和相對應前言間之適用關係。

In particular, according to article 70, (1) (e), the European Data Protection Board (hereafter 'EDPB') is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation and article 70, (1), (k) specifies the provision for guidelines concerning the setting of administrative fines.
尤其是，依據第70條第1項第e款，歐洲個人資料保護委員會（以下簡稱「EDPB」）有權

發布指引、建議和優良實務做法，以促進本規則適用之一致性，且第70條第1項第k款明定關於設定行政罰鍰之指引的規定。

These guidelines are not exhaustive, neither will they provide explanations about the differences between administrative, civil or criminal law systems when imposing administrative sanctions in general.

本指引並非詳盡無遺，且亦不會對行政、民事或刑事法律制度在一般課以行政處罰時之差異作出解釋。

In order to achieve a consistent approach to the imposition of the administrative fines, which adequately reflects all of the principles in these guidelines, the EDPB has agreed on a common understanding of the assessment criteria in article 83 (2) of the Regulation and therefore the EDPB and individual supervisory authorities agree on using this Guideline as a common approach.

為充分反映這些指引中之所有原則，以一致性之方式裁處行政罰鍰，EDPB已對本規則第83條第2項中之評估標準達成共識，因此EDPB和個別監管機關均同意以本指引作為共同的方法。

II. Principles
原則

Once an infringement of the Regulation has been established based on the assessment of the facts of the case, the competent supervisory authority must identify the most appropriate corrective measure(s) in order to address the infringement. The provisions of article 58 (2) b-j[1] indicate which tools the supervisory authorities may employ in order to address non-compliance from a controller or a processor. When using these powers, the supervisory authorities must observe the following principles:

一旦依據案件事實之評估而確認違反本規則，權責監管機關必須識別最合適之矯正措施以因應違反之情況。第58條第2項第b-j款[1]之規定表明監管機關可採用何種工具以因應控管者或受託運用者不合規之情形。當行使這些權力時，監管機關必須遵守以下原則：

1. *Infringement of the Regulation should lead to the imposition of "equivalent sanctions".*
   違反本規則應處以「同等之制裁」。

The concept of "equivalence" is central in determining the extent of the obligations of the supervisory authorities to ensure consistency in their use of corrective powers according to article 58 (2) in general, and the application of administrative fines in particular[2].

「同等」之概念於決定監管機關之責任範圍時為主要核心，以確保監管機關依據第58條第2項行使矯正權之一致性，尤其是行政罰鍰之適用範圍，[2]。

In *order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union,* ***the level of protection should be equivalent*** *in all Member States* (recital 10). Recital 11 elaborates the fact that an equivalent level of protection of personal data throughout the Union requires, amongst others, "*equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.*". Further more,

[1] Article 58 (2) a provides that warnings may be issued when "processing operations are likely to infringe provisions of the Regulation". In other words, in the case covered by the provision the infringement of the Regulation has not occurred yet.
第58條第2項第a款規定，當「運用作業可能違反本規則之條款」時，可發出警告。易言之，在該條款所涵蓋之範圍內，尚未發生違反本規則之情況。

[2] Even where the legal systems in some EU countries do not allow for the imposition of administrative fines as set out in the Regulation, such an application of the rules in those Member States needs to have an equivalent effect to administrative fines imposed by supervisory authorities (recital 151). The Courts are bound by the Regulation but they are not bound by these guidelines of the EDPB.
即使某些歐盟國家的法律制度不允許處以本規則所規定之行政罰鍰，惟當這些成員國適用該國法規時，仍需與監管機關得處以之行政罰鍰效果相當（前言第151點）。法院受本規則之約束，但不受這些EDPB指引之約束。

equivalent sanctions in all Member States as well as effective cooperation between supervisory authorities of different Member States is seen as a way "*to prevent divergences hampering the free movement of personal data within the internal market*", in line with recital 13 of the Regulation.

*為了確保對自然人一致性和高標準之保護，並移除歐盟境內個人資料流通之阻礙，所有成員國應提供**同等程度之保護**（前言第10點）*。前言第11點中亦詳述，對歐盟境內個人資料提供同等程度之保護須有「*同等程度之權力以監控和確保個人資料保護規則之遵守，以及成員國對違反行為有同等程度之制裁*」。此外，所有成員國之同等制裁以及不同成員國監管機關間之有效合作被視為係「*防止分歧阻礙個人資料在內部市場自由流通*」之方式，此與本規則前言第13點一致。

The Regulation sets a stronger basis than Directive 95/46/EC for a greater level of consistency as the Regulation is directly applicable in the Member States. While supervisory authorities operate with "complete independence" (article 52) with respect to national governments, controllers or processors, they are required to cooperate "*with a view to ensuring the consistency of application and enforcement of this Regulation*" (article 57, (1),(g)).

由於本規則可直接適用於成員國，因此本規則制定了比第95/46/EC號指令更強力之基礎，以實現更大程度之一致性。雖然監管機關作業「完全獨立」（第52條）於國家政府、控管者或受託運用者，然其被要求必須相互合作「*以確保本規則適用和執法之一致性*」（第57條第1項第g款）。

The Regulation calls for a greater consistency than the Directive 95/46 when imposing sanctions. In cross border cases, consistency shall be achieved primarily through the cooperation (one–stop-shop) mechanism and to some extent through the consistency mechanism set forth by the new Regulation.

在施以制裁時，本規則要求比第95/46號指令更大程度之一致性。就跨境案件而言，一致性應主要係透過合作（一站式）機制，並在一定程度上透過新規則所規定之一致性機制始得以實現。

In national cases covered by the Regulation, the supervisory authorities will apply these guidelines in the spirit of cooperation according to article 57, 1 (g) and article 63, with a view to ensuring the consistency of application and enforcement of the Regulation. Although supervisory authorities remain independent in their choice of the corrective measures presented in Article 58 (2), it should be avoided that different corrective measures are chosen by the supervisory authorities in similar cases.

就本規則所涵蓋之成員國案件而言，監管機關將依據第57條第1項第g款和第63條之合作精神適用這些指引，以確保本規則適用和執法之一致性。雖然監管機關在選擇第58條第2項

規定之矯正措施時仍保持獨立，但應避免監管機關在類似案件中，選擇不同之矯正措施。

The same principle applies when such corrective measures are imposed in the form of fines.
當以罰鍰形式執行此類矯正措施時，適用相同之原則。

---

2. Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive".
行政罰款與監管機關所選擇之所有矯正措施相同，必須「有效性、合比例性與具勸阻性」。

Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).
與一般所有矯正措施相同，行政罰鍰應足以反應侵害之性質、嚴重程度和後果，監管機關必須以一致且客觀合理之方式評估案件所有事實。在每個案件中，評估何者為有效性、合比例性與具勸阻性時，亦須反映所選擇之矯正措施追求的目標，即欲重新建立對規則之遵守，或欲處罰違法之行為（或兩者）。

Supervisory authorities should identify a corrective measure that is "*effective, proportionate and* dissuasive" (art. 83 (1)), both in national cases (article 55) and in cases involving cross- border processing of personal data (as defined in article 4 (23)).
監管機關應在成員國之案件（第55條）和涉及跨境運用個人資料之案件中（如第4條第23款之定義）識別出「*有效性、合比例性與具勸阻性*」之矯正措施（第83條第1項）。

These guidelines recognize that national legislation may set additional requirements on the enforcement procedure to be followed by the supervisory authorities. This may for example include address notifications, form, deadlines for making representations, appeal, enforcement, payment[3].
這些指引認識到國家立法可能對監管機關應遵循之執法程序設置額外要求。可能包括如：發出通知、格式、指定代理人期限、上訴、執行、支付[3]。

[3] As an example, the constitutional framework and draft data protection legislation of Ireland, provides that a formal decision is reached on the fact of the infringement itself, which is communicated to the relevant parties, before an assessment of the scale of the sanction(s). The decision on the fact of the infringement itself cannot be revisited during the assessment of the scale of the sanction(s).
例如，愛爾蘭的憲法框架和資料保護立法草案規定，在對制裁範圍進行評估前，須就違反事實本身作出正式決定，並將其傳達予相關各方。在評估制裁範圍時，不得重新審查違反事實本身之決定。

Such requirements should however not hinder in practice the achievement of effectiveness, proportionality or dissuasiveness.
然而，這些要求在實務上不應妨礙有效性、合比例性或具勸阻性之實現。

A more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities (on data protection, as well as lessons learned from other regulatory sectors) as well as case-law when interpreting these principles.
監管機關之實務做法（關於資料保護和從其他監管部門汲取之經驗）以及解釋這些原則之判例法，將對有效性、合比例性或具勸阻性產生更精準之判斷。

In order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU, namely that the concept of an undertaking **is understood to mean** an economic unit, which may be formed by the parent company and all involved subsidiaries. In accordance with EU law and case-law[4], an undertaking must be understood to be the economic unit, which engages in commercial/economic activities, regardless of the legal person involved (Recital 150).
為使裁處之罰鍰具有效性、合比例性與勸阻性，監管機關應使用歐盟法院為適用歐盟基本條約第101條和第102條之目的而對企業之概念所為之定義，即該企業之概念**應理解為**一個可由母公司和所有相關子公司組成之經濟單位。依據歐盟法律和判例法[4]，企業必須被理解為從事商業/經濟活動之經濟單位，無論是否涉及法人（前言第150點）。

---

3. *The competent supervisory authority will make an assessment "in each individual case".*
權責監管機關將「於每一個案件中」進行評估。

Administrative fines may be imposed in response to a wide range of infringements. Article 83 of the Regulation provides a harmonized approach to breaches of obligations expressly listed in paras (4)-(6). Member State law may extend the application of article 83 to public authorities

[4] The ECJ case law definition is: «the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed" (Case Höfner and Elsner, para 21, ECLI:EU:C:1991:161). An undertaking «must be understood as designating an economic unit even if in law that economic unit consists of several persons, natural or legal» (Case Confederación Española de Empresarios de Estaciones de Servicio [para 40, ECLI:EU:C:2006:784).
歐洲法院判例法之定義為：「企業之概念包括從事經濟活動的每個實體，無論該實體之法律地位及其融資方式為何」（CaseHöfner和Elsner，第21段，ECLI：EU：C：1991：161）。企業「必須被理解為一個指定的經濟單位，即使在法律定義下該經濟單位係由多人組成，無論是自然人或法人」（西班牙服務據點營運商聯合會案例，第40段，ECLI:EU:C:2006:784）。

and bodies established in that Member State. Additionally, Member State law may allow for or even mandate the imposition of a fine for infringement of other provisions than those mentioned in article 83 (4)-(6).

針對各種違反行為皆有處以行政罰鍰之可能。本規則第83條對違反第4 – 6項明確列舉之義務提供了一種一致性之處理方式。成員國法律可擴大第83條的適用範圍至設立於該成員國境內之公務機關和機構。此外，成員國法律可允許或甚至授權對於違反第83條第4 – 6項以外之其他規定處以罰鍰。

The Regulation requires assessment of each case individually[5]. Article 83 (2) is the starting point for such an individual assessment. The paragraph states "*when deciding whether to impose an administrative fine, and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…*"Accordingly, and also in the light of Recital 148[6] the supervisory authority has the responsibility of choosing the most appropriate measure(s). In the cases mentioned in Article 83 (4) – (6), this choice **must** include consideration of all of the corrective measures, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own.

本規則要求個別評估每一案件[5]。第83條第2項係此類個案評估之起始點。該項規定「*在決定是否處以行政罰鍰，且於個案中對行政罰鍰之金額作出決定時，應就以下要件給予適當之考量.....*」。因此，且依據前言第148點[6]，監管機關有責任選擇最合適之措施。在第83

[5] Further to the application of article 83 criteria there are other provisions to bolster the foundation of this approach such as:

除第83條標準之適用外，尚有其他條款支持此種方式之基礎，例如

- recital 141 "*the investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case.*"
  前言第141點「*申訴後之調查應在符合司法審查之具體個案的適當範圍中進行。*」
- recital 129 "*The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case…".*
  前言第129點「*監管機關權力之行使應依據歐盟和成員國法律所規定之適當程序性安全維護措施，在合理時間內以公平且公正之方式為之。尤其是，考量到每個案件的具體情況，為確保對本規則之遵守，每項措施皆應為適當的、必要的及合比例性…。*」
- article 57(1) (f) "*handle complaints lodged by a data subject, or by a body, organisation or association in accordance with article 8(應為第Article 80), and investigate to the extent appropriate, the subject matter of the complaint*."
  第57條第1項第f款「處理當事人或機構、組織或協會依據第80條提出之申訴，並在適當的範圍內調查該申訴事項。」

[6] "*In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory*

條第4－6項所提及之情況下，此種選擇**必須**包括考量所有矯正措施，其中包括考量單獨處以適當之行政罰鍰，或併行採取第58條第2項規定之矯正措施。

Fines are an important tool that supervisory authorities should use in appropriate circumstances. The supervisory authorities are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.

罰鍰係監管機關在適當情況下應使用之重要工具。鼓勵監管機關在實施矯正措施時採用經過深思熟慮且平衡之方式，以便達到對侵害行為施以有效性、具勸阻性以及合比例性之回應。關鍵為不將罰鍰視為最後手段，亦非避免罰鍰，但另一方面，罰鍰之使用不應減低其作為重要工具之有效性。

The EDPB, when competent according to article 65 of the Regulation, will issue a binding decision on disputes between authorities relating in particular to the determination of the existence of an infringement. When the relevant and reasoned objection raises the issue of the compliance of the corrective measure with the GDPR, the decision of EDPB will also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed in the draft decision of the competent supervisory authority. EDPB guidance on the application of article 65 of the Regulation will follow separately for further detail on the type of decision to be taken by the EDPB.

當符合本規則第65條之規定時，EDPB將就機關間，尤其是關於是否存在違反行為之爭議，做出具有約束力之決定。當對矯正措施是否符合GDPR提出相關及合理之異議時，EDPB亦將討論權責監管機關初步決定建議之行政罰鍰如何遵守有效性、合比例性與具勸阻性原則並做決定。EDPB關於適用本規則第65條之指導將另外進一步詳細說明EDPB可採取決定之類型。

---

authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process".

「*為加強本規則法規之執行，除了或代替監管機關依據本規則所採取之適當措施外，應對違反本規則之行為處以包括行政罰鍰等之處罰。若僅是輕微之違反或可能被處以之罰鍰對自然人構成不成比例之負擔時，得採用告誡之方式取代罰鍰。但應適當考量違反之性質、嚴重程度和持續期間、違反之故意性、為減輕所受損害而採取之行動、責任程度或先前任何相關之違反、監管機關獲知該違反行為之方式、遵守針對控管者或受託運用者之命令措施、遵守行為守則以及其他任何加重或減輕之要素。裁處包括行政罰鍰之處罰應遵守符合歐盟法及(歐洲聯盟基本權利憲章)憲章中一般原則之適當程序性安全維護措施，包括有效之司法保護及正當程序*」。

4. *A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among Supervisory Authorities*
為就資料保護領域之行政罰鍰採取協調一致之方法，需監管機關相互間之積極參與和資訊交流

These guidelines acknowledge that fining powers represent for some national supervisory authorities a novelty in the field of data protection, raising numerous issues in terms of resources, organization and procedure. Notably, the decisions in which the supervisory authorities exercise the fining powers conferred to them will be subject to appeal before national courts.
本指引承認，對某些國家監管機關而言，罰鍰權是資料保護領域的新穎經驗，且在資源、組織和程序方面引起了許多問題。值得注意的是，監管機關行使被賦予之罰鍰權而為之決定可上訴於國家法院。

Supervisory authorities shall cooperate with each other and where relevant, with the European Commission through the cooperation mechanisms as set out in the Regulation in order to support formal and informal information exchanges, such as through regular workshops. This cooperation would focus on their experience and practice in the application of the fining powers to ultimately achieve greater consistency.
監管機關應透過本規則規定之合作機制相互合作，且在需要時與歐盟執委會合作，並透過定期研討會等方式，以維持正式和非正式之資訊交流。此種合作將側重於監管機關在應用罰鍰權方面之經驗和實務做法，以最終實現更大程度之一致性。

This proactive information sharing, in addition to emerging case law on the use of these powers, may lead to the principles or the particular details of these guidelines being revisited.
此種主動的資訊共享，以及行使這些權力之新判例法，可能導致本指引之原則或具體細節被重新審視。

III. Assessment criteria in article 83 (2)
第83條第2項中之評估標準

Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine. This does not recommend a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case, as provided by article 83[7].
第83條第2項提供了監管機關在評估是否應處以罰鍰和罰鍰金額時應使用之標準清單。在此不建議相同標準之重複評估，而是建議依據第83條之規定，考量每一個案之所有情況[7]後之一次性評估。

The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice.
在第一階段評估中得出之結論可在關於罰鍰金額的第二階段中援用，從而避免使用相同之標準評估二次。

This section provides guidance for the supervisory authorities of how to interpret the individual facts of the case in the light of the criteria in article 83 (2).
本章節為監管機關提供指導，以瞭解如何依據第83條第2項之標準解釋案件之個別事實。

(a) the nature, gravity and duration of the infringement
違反之性質、嚴重程度和持續期間

Almost all of the obligations of the controllers and processors according to the Regulation are categorised according to their **nature** in the provisions of article 83(4) – (6). The Regulation, in setting up two different maximum amounts of administrative fine (10/20 million Euros), already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions. However the competent supervisory authority, by assessing the facts of the case in light of the general criteria provided in article 83 (2), may decide that in the particular case there is a higher or a more reduced need to react with a corrective measure in

[7] The assessment of the sanction to be applied may come separately after the assessment of whether there has been an infringement due to national procedural rules arising from constitutional requirements in some countries. Therefore, this may limit the content and the amount of detail in a draft decision issued by lead supervisory authority in such countries.
因某些國家憲法要求之國家程序法，對所適用制裁方法之評估，可能係於評估是否有違反行為之後，單獨進行。因此，可能會限制這些國家的主責監管機關發布草擬決定之內容和細節數量。

the form of a fine. Where a fine has been chosen as the one or one of several appropriate corrective measure(s), the tiering system of the Regulation (article 83 (4)- 83 (6)) will be applied in order to identify the maximum fine that can be imposed according to the nature of the infringement in question.
依據本規則，幾乎所有控管者和受託運用者之義務皆依據其**性質**，於第83條第4－6項中加以分類。本規則制定兩種不同之行政罰鍰金額上限（1/2千萬歐元），以指出違反本規則某些條款可能比違反其他條款更加嚴重。然而，權責監管機關在依據第83條第2項規定之一般標準評估案件事實時，可決定在特定個案中是否需要以裁處罰鍰形式作為矯正措施。當罰鍰被選擇為一種或其中一種適當的矯正措施時，將適用本規則之層級化體系（第83條第4項－83條第6項），以確認依據系爭違反性質可裁處之最高罰鍰金額。

Recital 148 introduces the notion of "minor infringements". Such infringements may constitute breaches of one or several of the Regulation's provisions listed in article 83 (4) or (5). The assessment of the criteria in article 83 (2) may however lead the supervisory authority to believe that in the concrete circumstances of the case, the breach for example, does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. In such cases, the fine may (but not always) be replaced by a reprimand.
前言第148點引進了「輕微違反」之概念。此類違反行為可能構成違反第83條第4項或第5項中所列一項或多項之規定。然而，第83條第2項之評估標準可能使監管機關認為，在案件的具體情狀下，例如，侵害行為未對相關當事人之權利造成重大風險，亦未影響系爭義務之實質面。在此類案件中，罰鍰或許（但非總是）可被告誡取代。

Recital 148 does not contain an obligation for the supervisory authority to always replace a fine by a reprimand in the case of a minor infringement ("*a reprimand may be issued instead of a fine*"), but rather a possibility that is at hand, following a concrete assessment of all the circumstances of the case.
前言第148點並無規定監管機關有義務在輕微違反之情況下必須以告誡取代罰鍰（「*可能予以告誡而非裁處罰鍰*」），而是對案件所有情狀具體評估後，一種可能之選擇。

Recital 148 opens up the same possibility to replace a fine by a reprimand, where the data controller is a natural person and the fine likely to be imposed would constitute a disproportionate burden. The starting point is that the supervisory authority has to assess whether, considering the circumstances of the case at hand, the imposition of a fine is required. If it finds in favour of imposing a fine, then the supervisory authority must also assess whether the fine to be imposed would constitute a disproportionate burden to a natural

person.
當資料控管者為自然人且可能被處以之罰鍰將造成不成比例之負擔時，前言第148點開啟了以告誡取代罰鍰之相同可能性。起始點仍為監管機關必須依據當前案件之情況，評估是否需處以罰鍰。若監管機關認為需處以罰鍰，則其亦必須評估所處以之罰鍰是否會對自然人構成不成比例之負擔。

Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case.
本規則並未對特定違反行為給予具體之價格標籤，而只定有上限（最高金額）。相較於第83條第5項，對第83條第4項所列義務之違反，嚴重程度相對較低。然而，就違反第83條第5項所為之有效性、符合比例性與具勸阻性之回應方式，仍將取決於案件之具體情況。

It should be noticed that breaches of the Regulation, which by their nature might fall into the category of "up to 10 million Euros or up to 2% of total annual worldwide turnover" as set out in article 83 (4), might end up qualifying for a higher tier (Euro 20 million) category in certain circumstances. This would be likely to be the case where such breaches have previously been addressed in an order from the supervisory authority, an order[8] which the controller or processor failed to comply with[9] (article 83 (6)). The provisions of the national law may in practice have an impact on this assessment[10]. The nature of the infringement, but also "*the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them*", will be indicative of the **gravity** of the infringement. The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12. More detail at this stage is beyond the scope of this particular guideline (as detailed calculation work would be the focus of a potential subsequent stage of this guideline).
應注意的是，違反本規則之行為，依其性質，可能落入第83條第4項規定「最高1000萬歐元或全球年度總營業額2%」之類別，在某些情況下，亦可能被歸類於更高金額（2000

萬歐元）之類別。此種情況很可能是監管機關已於先前之命令[8]中指出了此種違反行為，而控管者或受託運用者未能遵守其命令[9]（第83條第6項）。國家法律規定實際上可能會對此一評估產生影響[10]。違反之性質，以及「*相關運用之範圍和目的、受影響當事人之人數以及當事人受損害之程度*」，皆能指出違反之**嚴重程度**。在任何特定案件中同時發生若干不同違反行為時，監管機關得在最嚴重之違反行為的限制範圍內裁處有效性、合比例性與具勸阻性之行政罰鍰。因此，若發現違反第8條和第12條之行為，則監管機關可採取第83條第5項規定之矯正措施，以因應第12條所列之最嚴重違反行為種類。本階段之進一步細節已超出本指引之範圍（詳盡之計算工作將係本指引可能之後續階段重點）。

The factors below should be assessed in combination eg. the number of data subjects together

---

[8] The orders, provided in article 58 (2) are:
第58條第2項規定之命令為：

- to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
  命令控管者或受託運用者遵守當事人依據本規則行使其權利之要求；
- to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
  命令控管者或受託運用者，如適當，以特定方式並在規定期限內使運用作業符合本規則之規定；
- to order the controller to communicate a personal data breach to the data subject;
  命令控管者將個人資料侵害資訊傳達予當事人；
- to impose a temporary or definitive limitation including a ban on processing
  施以臨時或最終之限制，包括禁止運用
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
  依據第16、17和18條命令更正或刪除個人資料或限制運用，並依據第17條第2項和第19條向被揭露個人資料之接收者發出此類行動之通知；
- to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
  命令認證機構撤銷依據第42條和第43條核發之認證，或命令認證機構不得核發認證，若未能滿足或不再符合認證要求。
- to order the suspension of data flows to a recipient in a third country or to an international organisation.
  命令暫停資料傳輸至第三國之接收者或國際組織。

[9] Application of article 83(6) necessarily must take into account national law on procedure. National law determines how an order is issued, how it is notified, from which point it takes effect, whether there is a grace period to work on compliance. Notably, the effect of an appeal on the enforceability of an order should be taken into account.
第83條第6項之適用於程序上必須考量到國家法律。國家法律決定命令如何發布、如何通知、從何時起生效、是否存在合規性之寬限期。值得注意者為，應考量上訴對命令可執行性之影響。

[10] Statutory provisions of limitation may have the effect that a previous order of the supervisory authority may no longer be taken in to consideration due to the amount of time that has lapsed since that previous order was issued. In some jurisdictions, rules require that after the prescription period has passed with respect to an order, no fine may be imposed for non-compliance with that order under article 83(6). It will be up to each supervisory authority in each jurisdiction to determine how such impacts will affect them.
法定限制條款可能會導致不須考量監管機關先前之命令，因該命令自發布以來已經過一定之時間。在某些管轄權內，法規要求當命令之時效經過後，對於不遵守第83條第6項下之命令不得處以罰鍰。此將由每一管轄權內之每個監管機關來認定這些衝突對其自身之影響。

with the possible impact on them.
以下因素應結合評估，例如，當事人之人數以及可能對其產生之影響。

The number of data subjects involved should be assessed, in order to identify whether this is an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place. This is not to say that isolated events should not be enforceable, as an isolated event could still affect a lot of data subjects. This will, depending on the circumstances of the case, be relative to, for example, the total number of registrants in the database in question, the number of users of a service, the number of customers, or in relation to the population of the country, as appropriate.
應評估所涉及當事人之人**數**，以辨別此為獨立事件，或是系統性侵害的徵兆，或缺乏適當常規程序。此非謂不可對獨立事件執法，因單一事件仍可影響許多當事人。依據案件具體情況，此將與，例如，系爭資料庫註冊者總數、一項服務的用戶數量、消費者數量相關，或於適當情況下，與國家人口數相關。

The purpose of the processing must also be assessed. The WP 29 opinion on "purpose limitation"[11] previously analysed the two main building blocks of this principle in data protection law: purpose specification and compatible use. When assessing the purpose of the processing in the context of article 83 (2), the supervisory authorities should look into the extent to which the processing upholds the two key components of this principle[12]. In certain situations, the supervisory authority might find it necessary to factor in a deeper analysis of the purpose of the processing in itself in the analysis of article 83 (2).
運用之**目的**亦須被納入評估。29條工作小組先前關於「目的限制」[11]之意見分析了資料保護法中此一原則的兩個主要組成部分：目的明確性和用途相容性。在第83條第2項範圍內評估運用目的時，監管機關應考量該運用在多大程度上可維護本原則的兩個關鍵組成部分[12]。在特定情況下，監管機關可能發現有必要在分析第83條第2項時更深入地解析運用本身之目的。

If the data subjects have suffered **damage**, the level of the damage has to be taken into consideration. Processing of personal data may generate risks for the rights and freedoms of

[11] WP 203 , Opinion 03/2013 on purpose limitation, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
第03/2013號意見，關於目的限制，WP 203，請查詢 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf。

[12] See also WP 217, opinion 6/2014 on the notion of legitimate interest of the data controller under article 7, page 24, on the question: "What makes an interest "legitimate" or "illegitimate"?"
另請參閱，第6/2014號意見，關於第7條資料控管者正當利益之概念，WP 217，第24頁，關於：「什麼使利益『正當』或『不正當』?」之問題。

the individual, as illustrated by recital 75:

若當事人遭受**損害**，則必須考量其損害程度。運用個人資料可能會對當事人之權利和自由產生風險，如前言第75點所述：

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non- material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."*
>
> *「個人資料運用可能導致自然人的權利及自由產生不同可能性與嚴重性的風險，恐造成人身、財物或非財物的損害，尤其是：在運用可能導致歧視、身分冒用或詐欺、財務損失、聲譽受損、受職業秘密保護的個人資料之秘密性喪失、未經授權的假名化回溯、或任何其他重大經濟性或社會性之不利益時；在當事人可能被剝奪其權利和自由或被禁止對其個人資料行使控制權時；在運用個人資料將揭露種族或民族、政治觀點、宗教或哲學信仰、工會會員資格、基因資料運用、健康資料或有關性生活或刑事前科和犯罪或相關安全措施之資料時；在涉及評估個人面向，尤其是分析或預測有關工作表現、經濟情況、健康、個人偏好或興趣、可靠性或行為、所在位置或移動，以建立或使用個人資料檔案時；在運用弱勢自然人，尤其是兒童之個人資料時；或在運用涉及大量個人資料並影響大量當事人時。」*

If damages have been or are likely to be suffered due to the infringement of the Regulation

then the supervisory authority should take this into account in its choice of corrective measure, although the supervisory authority itself is not competent to award the specific compensation for the damage suffered.
若因違反本規則而已經或可能受到損害，則監管機關在選擇矯正措施時應就此情形加以考量，儘管監管機關本身並無權就所遭受之損害給予具體賠償。

The imposition of a fine is not dependent on the ability of the supervisory authority to establish a causal link between the breach and the material loss (see for example article 83 (6)).
罰鍰之課處並不取決於監管機關在侵害和實質損害間建立因果關係之能力（請參閱例如第83條第6項）。

Duration of the infringement may be illustrative of, for example:
違反之**持續期間**可說明，例如：

a) wilful conduct on the data controller's part, or
資料控管者之故意行為，或

b) failure to take appropriate preventive measures, or
未採取適當之預防措施，或

c) inability to put in place the required technical and organisational measures.
無能力實施所需之技術性和組織性措施。

(b) the intentional or negligent character of the infringement
違反行為之故意或過失

In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.
一般說來，「故意」包含對違法行為相關要素之知悉和意欲，而「非故意」意味著雖然控管者/受託運用者違反了法律規定之注意義務，然卻無意造成該違反行為。

It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered

from the facts of the case. In addition, emergent case law and practice in the field of data protection under the application of the Regulation will be illustrative of circumstances indicating clearer thresholds for assessing whether a breach was intentional.
一般普遍承認，故意違法，表示對法律規定之蔑視，比非故意違法更為嚴重，因此更有可能被處以行政罰鍰。其結果為故意或過失，將以該案件事實之行為客觀要素判斷。此外，就本規則之適用，資料保護領域下之新判例法和實務作法將在評估是否為故意違法時，提供更明確之門檻。

Circumstances indicative of intentional breaches might be unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies, for example obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market.
認定為故意違反之情狀可能包含來自於控管者最高管理層級明確授權之非法運用，或儘管個資保護長已提出建議或根本無視現有政策，例如意圖使市場上的競爭對手失去信譽而取得及運用競爭對手之員工資料。

Other examples here might be:
其他之示例可能為：

- amending personal data to give a misleading (positive) impression about whether targets have been met – we have seen this in the context of targets for hospital waiting times
  修改個人資料，以對是否達成目標做出誤導性（積極）之印象–我們曾在關於「醫院候診時間之目標」見到此種情況。

- the trade of personal data for marketing purpose ie selling data as ‘opted in’ without checking/disregarding data subjects’ views about how their data should be used
  基於行銷目的交易個人資料，即未檢視/漠視當事人關於如何使用其資料之觀點，預設當事人選擇同意出售資料。

Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them)may be indicative of negligence.
其他情狀，例如未能閱讀和遵守現有政策、人為錯誤、未能檢查公布資訊中之個人資料、

未能及時實施技術性更新、未能採行政策（而非單純的不加以應用），可能認定為過失。

Enterprises should be responsible for adopting structures and resources adequate to the nature and complexity of their business. As such, controllers and processors cannot legitimise breaches of data protection law by claiming a shortage of resources. Routines and documentation of processing activities follow a risk-based approach according to the Regulation.
企業應有責任採行適合其業務性質和複雜性之結構及資源。因此，控管者和受託運用者不得藉由聲稱資源短缺以正當化其違反資料保護法之行為。運用活動之例行程序和文件記錄須依據本規則以風險為基礎之方式為之。

There are grey areas which will affect decision-making in relation to whether or not to impose a corrective measure and the authority may need to do more extensive investigation to ascertain the facts of the case and to ensure that all specific circumstances of each individual case were sufficiently taken into account.
某些灰色地帶會影響是否採取矯正措施之決定，而機關可能需要進行更廣泛之調查，以確認案件事實，並確保充分考量到每個案件的所有具體情況。

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
控管者或受託運用者為減輕當事人所遭受之損害而採取的任何行動；

The data controllers and processors have an obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising form the processing of personal data to the rights and freedoms of the individuals. However, when a breach occurs and the data subject has suffered damage, the responsible party should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the supervisory authority in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case.
資料控管者和受託運用者有義務實施技術性和組織性措施，以確保適合風險之安全層級、辦理個資保護影響評估、並減輕運用個人資料對當事人權利和自由所造成之風險。然而，若發生侵害且當事人受到損害時，責任方應該盡其所能，以減輕該侵害行為對相關當事人之後果。監管機關在選擇矯正措施以及計算特定案件中之懲罰金額時，將考量此種負責任（或不負責任）之行為。

Although aggravating and mitigating factors are particularly suited to fine-tune the amount of a fine to the particular circumstances of the case, their role in the choice of appropriate corrective measure should not be underestimated. In cases where the assessment based on other criteria leaves the supervisory authority in doubt about the appropriateness of an administrative fine, as a standalone corrective measure, or in combination with other measures in article 58, such aggravating or attenuating circumstances may help to choose the appropriate measures by tipping the balance in favour of what proves more effective, proportionate and dissuasive in the given case.

雖然加重和減輕因素特別適合於依據案件之特定情況微調罰鍰金額，但不應低估其在選擇適當矯正措施中之作用。若基於其他標準的評估使監管機關對行政罰鍰之適當性有疑義時，例如應採一項單獨之矯正措施或併同第58條中其他措施，在特定案件中，此種加重或減輕情形藉由衡量哪種措施較有效性、合比例性與具勸阻性，可能有助於適當措施之選擇。

This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.

本條款作用在違反行為發生後，對控管者責任程度之評估。該條款可能涵蓋當控管者/受託運用者顯然沒有重大過失/過失之作為，且在意識到侵害發生時，已盡其所能改正其行為之情況。

Regulatory experience from SAs under the 95/46/EC Directive has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions. This might include examples such as (although this would not lead to a more flexible approach in every case):

監管機關先前在第95/46/EC號指令下之SA監管經驗已顯示出，對於已承認違反行為，並負責改正或限縮其行為所造成之影響的資料控管者/受託運用者，表現出某種程度之彈性是適當的。此可能包括之示例如（雖然這不會導致每個案件都適用更彈性方式）：

- contacting other controllers/processors who may have been involved in an extension of the processing e.g. if there has been a piece of data mistakenly shared with third parties.

  聯繫可能涉及延伸運用之其他控管者/受託運用者，例如曾誤與第三方分享一些資料。

- timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did.
  資料控管者/受託運用者即時採取行動，以阻止侵害繼續或擴大至產生更嚴重影響之程度。

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
控管者或受託運用者之責任程度，需考量到其依據第25條和第32條所執行之技術性和組織性措施；

The Regulation has introduced a far greater level of accountability of the data controller in comparison with the EC Data Protection Directive 95/46/EC.
與第95/46/EC號資料保護指令相較，本規則就資料控管者之課責性採用更高層級之規定。

The degree of responsibility of the controller or processor assessed against the backdrop of applying an appropriate corrective measure may include:
以採行適當矯正措施為背景評估控管者或受託運用者之責任程度，可能包括：

- Has the controller implemented technical measures that follow the principles of data protection by design or by default (article 25)?
  控管者是否已執行符合資料保護設計或預設原則之技術性措施（第25條）？
- Has the controller implemented organisational measures that give effect to the principles of data protection by design and by default (article 25) at all levels of the organisation?
  控管者是否已在組織內各個層級皆已執行資料保護設計或預設原則之組織性措施（第25條）？
- Has the controller/processor implemented an appropriate level of security (article 32)?
  控管者/受託運用者是否已落實適當之安全程度（第32條）？
- Are the relevant data protection routines/policies known and applied at the appropriate level of management in the organisation? (Article 24).
  組織之適當管理層級是否已知曉並適用相關資料保護例行程序/政策？（第24條）。

Article 25 and article 32 of the Regulation require that the controllers "*take into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms for the natural persons posed by the processing*". Rather than being an obligation of goal, these provisions introduce obligations of means, that is, the controller must make the necessary assessments and reach the appropriate conclusions. The question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation.

本規則第25條和第32條要求控管者「*考量現有技術、執行成本和運用之性質、範圍、背景與目的，以及運用對自然人權利和自由所造成風險之各種不同可能性和嚴重性*」。這些規定並非目標式之義務，而係引進方法式之義務，即控管者必須進行必要之評估並得出適當之結論。因此，監管機關必須回答的問題為，依本規則賦予之義務，於何種程度可認控管者依運用之性質、目的或規模「已做到其所被期待做到的事情」。

In this assessment, due account should be taken of any "best practice" procedures or methods where these exist and apply. Industry standards, as well as codes of conduct in the respective field or profession are important to take into account. Codes of practice might give an indication as to what is common practice in the field and an indication of the level of knowledge about different means to address typical security issues associated with the processing.

在本評估中，應適當考量現有和適用之任何「最佳實務」程序或方法。產業標準以及各別領域或專業中之行為守則係重要之考量因素。實務守則可提供某個領域中通用做法指標，及以不同方法解決與運用相關之典型安全議題之認知程度指標。

While best practice should be the ideal to pursue in general, the special circumstances of each individual case must be taken into account when making the assessment of the degree of responsibility.

一般來說，雖然最佳實務做法應是追求之理想，但在評估責任程度時，必須考量每個案件之特殊情況。

(e) any relevant previous infringements by the controller or processor;

控管者或受託運用者先前任何相關之違反行為；

This criterion is meant to assess the track record of the entity committing the infringement. Supervisory authorities should consider that the scope of the assessment here can be quite

wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be "relevant" for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.
本標準旨在評估實體違反行為之追蹤記錄。監管機關應考量到此處之評估範圍可能是非常廣泛的，因任何違反本規則之行為，即便性質可能與監管機關正在調查者不同，惟因其可顯示未充分知悉或未注意資料保護規則之總體情況，因此，仍可能與該評估「相關」。

The supervisory authority should assess:
監管機關應評估：

- Has the controller/processor committed the same infringement earlier?
  控管者/受託運用者過去是否曾犯過相同之違反行為？
- Has the controller/processor committed an infringement of the Regulation in the same manner? (for example as a consequence of insufficient knowledge of existing routines in the organisation, or as a consequence of inappropriate risk assessment, not being responsive to requests from the data subject in a timely manner, unjustified delay in responding to requests and so on).
  控管者/受託運用者是否以同樣之方式違反了本規則？（例如，由於對組織中現有慣例之認知不足，或由於不適當之風險評估、未能即時回應當事人之要求、對要求不合理的延遲回應等）。

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
與監管機關之配合程度，以補救違反行為並減輕其可能產生之不利影響；

Article 83 (2) provides that the degree of cooperation may be given "due regard" when deciding whether to impose an administrative fine and in deciding on the amount of the fine. The Regulation does not give a precise answer to the question how to take into account the efforts of the controllers or the processors to remedy an infringement already established by the supervisory authority. Moreover, it is clear that the criteria would usually be applied when calculating the amount of the fine to be imposed.
第83條第2項規定，在決定是否處以行政罰鍰和決定罰鍰金額時，可「適當考量」配合程度。就如何考量控管者或受託運用者為補救經監管機關確認之違反行為所做的努力之問題，本規則並未提供明確答案。此外，很明顯的，在計算課處之罰鍰金額時通常會適

用此標準。

However, where intervention of the controller has had the effect that negative consequences on the rights of the individuals did not produce or had a more limited impact than they could have otherwise done, this could also be taken into account in the choice of corrective measure that is proportionate in the individual case.
然而，若控管者之干預所造成之影響並未對當事人權利產生負面後果或產生比預期更有限之影響，在個案中選擇合比例性之矯正措施時，亦可納入考量。

One example of a case where cooperation with the supervisory authority might be relevant to consider might be:
考慮與監管機關配合之可能相關示例為：

- Has the entity responded in a particular manner to the supervisory authority's requests during the investigation phase in that specific case which has significantly limited the impact on individuals' rights as a result?
  在特定案件的調查階段，該實體是否以特別之方式回應監管機關之要求，從而大幅度限縮了對個人權利之影響？

This said, it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspections.
意即，對於法律已要求之配合並不適宜給予額外之關注，例如，在任何情況下，實體本需允許監管機關進入其營業處所進行稽核/檢查。

(g) the categories of the personal data affected by the infringement;
受違反行為影響之個人資料類型；

Some examples of key questions that the supervisory authority may find it necessary to answer here, if appropriate to the case, are:
若於該案件適合之情形，監管機關可能認為有必要回答之關鍵問題示例為：

- Does the infringement concern processing of special categories of data set out in articles 9 or 10 of the Regulation?
  違反行為是否涉及運用本規則第9條或第10條規定之特種資料？

- Is the data directly identifiable/ indirectly identifiable?
  資料是否可直接/間接識別？

- Does the processing involve data whose dissemination would cause immediate damage/distress to the individual (which falls outside the category of article 9 or 10)?
  運用是否涉及散播會對個人造成直接損害/痛苦之資料（並非屬第9條或第10條之類型）？

- Is the data directly available without technical protections, or is it encrypted[13]?
  資料是否無技術性保護而可直接使用，或者已加密[13]？

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

監管機關得知違反行為之方式，尤其係控管者或受託運用者是否就該違反行為進行通知以及通知之程度為何；

A supervisory authority might become aware about the infringement as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller. The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.

監管機關可能透過調查、申訴、新聞文章、匿名舉報或資料控管者之通知得知違反行為。依據本規則，控管者有義務向監管機關通知個人資料侵害事件。若控管者僅履行此義務，尚不得將遵守該義務解釋為減弱/減輕因素。同樣的，若資料控管者/受託運用者由於不注意而未能通知，或由於沒有充分評估違反行為之程度而未能通知違反行為之所有細節時，監管機關可考量較嚴厲之懲罰，即不太可能被歸類為輕微之違反行為。

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

若先前已基於相同爭議，向該控管者或受託運用者就第58條第2項所述措施發布命

[13] It shouldn't always be considered 'a bonus' mitigating factor that the breach only concerns indirectly identifiable or even pseudonymous/encrypted data. For those breaches, an overall assessment of the other criteria might give a moderate or strong indication that a fine should be imposed.
即使侵害僅涉及可間接識別之資料或甚至為假名化/加密資料，此情形不應被視為一種「紅利」減輕要素。對於這些侵害行為，其他標準之總體評估可能會得出適度或強烈之指標，顯示應處以罰鍰。

令，其遵循該措施之情形如何；

A controller or processor may already be on the supervisory authority's radar for monitoring their compliance after a previous infringement and contacts with the DPO where they exist are likely to have been extensive. Therefore, the supervisory authority will take into account the previous contacts.
在先前之違反行為後，監管機關可能已在雷達上監控控管者或受託運用者的法遵情形，並與個資保護長（如有）密切聯繫。因此，監管機關將考量先前之聯繫狀況。

As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors "*with regard to the same subject matter*".
與第（e）項中之標準相反，此評估標準之目的僅為提醒監管機關考量其先前已向同一控管者或受託運用者「*基於相同爭議*」所實施之措施。

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;
遵守依據第40條認可之行為守則或依據第42條認可之認證機制；

Supervisory authorities have a duty to "*monitor and enforce the application of this* Regulation, (article 57 1 (a))". Adherence to approved codes of conduct may be used by the controller or processor as an way to demonstrate compliance, according to articles 24 (3), 28 (5) or 32 (3).
監管機關有責任「*監督和執行本規則之適用*（第57條第1項第a款）」。依據第24條第3項、第28條第5項或第32條第3項，控管者或受託運用者可使用經認可之行為守則作為證明其合規性之方式。

In case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority. Approved codes of conduct will, according to article 40 (4) contain "*mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions*".
當違反本規則之其中一項規定時，依據已認可的行為守則，可能會使監管機關需要全面的採取有效性、合比例性與具勸阻性的行政罰款或其他糾正措施介入干預。依據第40條第4項，經認可之行為守則將包含「*相關機制使（監督）機構得對遵守其規定進行強制性之監督*」。

Where the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are "*without prejudice to the tasks and powers of the competent supervisory authority*", which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.

當控管者或受託運用者遵守經認可之行為守則時，監管機關或許可信賴負責管理守則之守則社群對其成員採取適當之行動，例如透過對行為守則本身之監督和執行計畫。因此，監管機關可能會認為這些措施於該特定情況下是屬有效性、合比例性或具勸阻性，而無需由監管機關本身施以額外之措施。依據第41條第2項第c款及42條第4項，可透過監督計畫對違規行為處以某些形式之懲罰，包括暫停或取消相關控管者或受託運用者於守則社群之資格。然而，監督機構之權力「*不得損害權責監管機關之任務和權力*」，此意味著監管機關並無義務考量自我監督計畫先前所實施之懲罰。

Non-compliance with self-regulatory measures could also reveal the controller's/processor's negligence or intentional behaviour of non-compliance.

不遵守自我監督措施亦可顯示控管者/受託運用者之過失或故意不遵守之行為。

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

適用於案件情狀之任何其他加重或減輕因素，例如直接或間接從違反行為中獲得經濟利益或避免損失。

The provision itself gives examples of which other elements might be taken into account when deciding the appropriateness of an administrative fine for an infringement of the provisions mentioned in Article 83(4-6).

該條款本身舉例說明了在決定因違反第83條第4-6項所述條款，而處以行政罰鍰之適當性時，可將其他因素納入考量。

Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.

因侵害而獲利之資訊對於監管機關而言可能尤其重要，因違反行為帶來的經濟利益無法透過非金錢之措施得到補償。因此，控管者從違反本規則中獲利之事實可能成為應處以罰鍰之強大指標。

IV. Conclusion
結論

Reflections on the questions such as those provided in the previous section will help supervisory authorities identify, from the relevant facts of the case, those criteria which are most useful in reaching a decision on whether to impose an appropriate administrative fine in addition to or instead of other measures under Article 58. Taking into account the context provided by such assessment, the supervisory authority will identify the most effective, proportionate and dissuasive corrective measure to respond to the breach.
對上述章節所提供問題之反思將有助於監管機關從案件的相關事實中識別出最有效用之標準，以決定在除了或替代第58條所規定其他措施之情況下，是否處以適當之行政罰鍰。考量此類評估所提供之脈絡，監管機關將識別出最有效性、合比例性與具勸誡性之矯正措施，以回應違反行為。

Article 58 provides some guidance as to which measures a supervisory authority might choose, as the corrective measures in themselves are different in nature and suited primarily for achieving different purposes. Some of the measures in article 58 may even be possible to cumulate, therefore achieving a regulatory action comprising more than one corrective measure.
第58條就監管機關可選擇之措施提供了一些指導，因矯正措施本身性質之不相同，且根本上適合不同目的之達成。第58條中所列舉之某些措施甚至可疊加適用，因此實現了包含一種以上矯正措施之監管行動。

It is not always necessary to supplement the measure through the use of another corrective measure. For example: The effectiveness and dissuasiveness of the intervention by the supervisory authority with its due consideration of what is proportionate to that specific case may be achieved through the fine alone.
並非總是需要使用另一措施來補充矯正措施。例如：監管機關以比例性適當考量特定案件情況，可能僅須透過罰鍰即可使干預行為具有效性及勸阻性。

In essence, authorities need to restore compliance through all of the corrective measures available to them. Supervisory authorities will also be required to choose the most appropriate channel for pursuing regulatory action. For example, this could include penal sanctions (where these are available at national level).
原則上，機關需透過所有可使用之矯正措施以恢復合規性。監管機關亦將被要求選擇最適合採取之監管行動管道。例如，此可能包括刑事處分（當此規範於成員國國內法時）。

The practice of applying administrative fines consistently across the European Union is an evolving art. Actions should be taken by supervisory authorities working together to improve consistency on an ongoing basis. This can be achieved through regular exchanges through case-handling workshops or other events which allow the comparison of cases from the sub-national, national and cross-border levels. The creation of a permanent sub-group attached to a relevant part of the EDPB is recommended to support this ongoing activity.

於歐盟內實施一致性行政罰鍰之做法仍是一門持續發展的藝術。監管機關應採取行動，共同努力，在現有基礎上不斷提升一致性。此可透過案件處理研討會或其他活動進行定期交流得以實現，這些活動可對來自地方、國家和跨境層級之案例進行比較。建議成立一個隸屬於EDPB相關部門之永久性小組以支援此項持續進行之活動。