「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：理律法律事務所

中華民國 111 年 12 月

「GDPR 相關指引文件研析」委託研究計畫

結案報告

受託單位：理律法律事務所

研究主持人：曾更瑩律師

協同主持人：蕭秀玲律師

計畫期程：中華民國 111 年 8 月至 111 年 12 月

國家發展委員會

中華民國 111 年 12 月

本研究報告內容僅供本會業務參考

摘要

自歐盟一般資料保護規則（General Data Protection Regulation, GDPR）於 2018 年 5 月 25 日施行以來，歐盟個人資料保護委員會（European Data Protection Board, EDPB）陸續發布 GDPR 相關指引文件進一步闡釋或舉例說明 GDPR 相關條文之具體適用情形，以利歐盟成員國及相關企業遵循。

無論是我國向歐盟申請適足性認定（Adequacy Decision），或我國企業及政府機關於適用 GDPR 之必要範圍內，均有進一步瞭解 GDPR 相關指引文件內容之必要，俾使我國對於個人資料保護及合理利用之法制與國際立法趨勢接軌。

為此，國家發展委員會特挑選四份 GDPR 相關指引文件，涵蓋個人資料侵害事故通報、控管者與受託運用者概念區分、被遺忘權於搜尋引擎案例適用判準、當事人近用權四大主題，除提出研析報告外，並將其譯為中文，供各界參考。

Abstract

Since the General Data Protection Regulation (GDPR) came into force on May 25, 2018, the European Data Protection Board (EDPB) has been publishing guidance documents on the GDPR to further explain or provide examples of the application of the relevant provisions of the GDPR to facilitate compliance thereof by EU member states and relevant enterprises.

Whether it is Taiwan's application to the EU for an Adequacy Decision, or the application of the GDPR by Taiwanese enterprises and government agencies to the extent necessary, it is necessary to further understand the content of the relevant guidance documents of the GDPR so that Taiwan's legal system for the protection and reasonable use of personal data is in line with the international legislative trends.

To this end, the National Development Council has selected four GDPR guidlines, covering the following four key topics: personal data breach notification, distinction between the concepts of controller and processor in the GDPR, criteria of the right to be forgotten in search engines cases, and data subjects' right of access, and arranged for a research analysis report as well as the Chinese translation thereof for the reference of the relevant stakeholders.

目錄

第一章 個人資料侵害事件通報範例指引（Guidelines 01/2021）.....1

第一節 簡介.....1

第二節 內容摘要.....2

第三節 與我國個人資料保護法之重點比較.....15

第四節 小結.....20

第二章 GDPR 控管者與受託運用者概念指引（Guidelines 07/2020）.....23

第一節 簡介.....23

第二節 內容摘要.....23

第三節 與我國個人資料保護法之重點比較.....32

第四節 小結.....38

第三章 GDPR 被遺忘權於搜尋引擎案例適用標準之指引（Guidelines 5/2019）.....41

第一節 簡介.....41

第二節 內容摘要.....42

第三節 與我國個人資料保護法之重點比較.....46

第四節 小結.....57

第四章 當事人權利（近用權）指引（Guidelines 01/2022）.....61

第一節 簡介.....61

第二節 內容摘要.....62

第三節 與我國個人資料保護法之重點比較.....77

第四節 小結.....83

第五章 指引翻譯.....86

第一章 個人資料侵害事件通報範例指引（Guidelines 01/2021）[1]

第一節 簡介

「個人資料侵害事件通報範例指引」（下稱事故通報指引）旨在釐清一般資料保護規則（General Data Protection Regulation，下稱GDPR）[2]第33條及第34條提及之個人資料侵害事件通報義務與程序，並針對「2016/679規則個人資料侵害事件通報指引」（Guidelines on Personal data breach notification under Regulation 2016/679, WP250）（下稱第WP250號指引）未就所有實務議題提供詳細說明處進行補充，透過提供案例說明方式彌補前述規定中未臻明確的部分。

事故通報指引透過將個人資料侵害事件類型化，藉以討論不同個人資料侵害事件當中，可能涉及的風險類型、如何評估風險與應考量何種因素等，並針對同一類型個人資料侵害事件中，因各種具體案例事實而可能產生的不同變化與最終導致的不同程度風險作進一步分析。事故通報指引針對不同的風險屬性和等級，分別從三個可能需要採取的行動（包含：備置內部紀錄、通報監管機關、通知當事人）出發，依據風險屬性給出建議執行之措施。事故通報指引於不同的個人資料侵害事件中，鑒於不同的風險等級，提出三種行動均無須採取、三種行動得選擇採用其一或其二，者三種行動皆須採用之不同建議。

事故通報指引主要是為建構一個以實務操作為導向、案例為基礎的指引，透過提出可能發生之個人資料侵害事件的案例，針對個案內容加以調整並進行假設，以利協助控管者瞭解在不同情形下，個人資料侵害事件產生的風險等級為何及風險評估時該考量之因素，最終歸納出如何因應個人資料侵害事件（包含三種常見的行動措施以及針對個別個人資料侵害事件可以採取的緩解措施），俾供各歐盟成員國主管機關參考。

---

[1] European Data Protection Board (EDPB), '*GUIDELINES 01/2021 ON EXAMPLES REGARDING PERSONAL DATA BREACH NOTIFICATION*', 14 December 2021 (Version 2.0).

[2] 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).

本文將先於第二節介紹GDPR對於個人資料侵害事件的三層次定義，再說明GDPR及第WP250號指引之相關規定，最後回歸事故通報指引，介紹在事故通報指引中，歐盟的規範制定者提出何種類型的個人資料侵害事件作為參考，以及針對各類型個人資料侵害事件，歐盟主管機關傾向如何判斷風險等級以及需要採取的措施。本文第三節將簡介我國現行法針對個人資料侵害（外洩）事件的處理規範，並分析我國法與GDPR在規範框架設計上的差異，比較何種規範方式可能較適合處理個人資料侵害事件。最終，本文將於第四節建議我國法可能之修改方向。

第二節 內容摘要

鑒於歐盟法下針對個人資料侵害事件的原則性規範係規定於GDPR及第WP250號指引，本節將先介紹這二個規範，以劃定歐盟法對於個人資料侵害事件的主要概念與相關規定，再透過事故通報指引進行案例式之補充說明與風險性評估。

一、GDPR與第WP250號指引中相關規定

(一) 個人資料侵害事件之三層次定義[3]

個人資料侵害事件可依據下列三項公認之安全性原則進行分類：「機密性」侵害事件－個人資料遭未經授權或意外之揭露或存取；「完整性」侵害事件－個人資料遭未經授權或意外之竄改；「可用性」侵害事件－個人資料本身或其存取途徑遭未經授權或意外之滅失或破壞。

(二) GDPR之要求

GDPR第4(12)條將「個人資料侵害事件」定義為「導致經傳輸、儲存或以其他方式運用之個人資料遭意外或非法破壞、滅失、竄改、

[3] EDPB, *supra* note 1, at 6.

未經授權揭露或存取之安全性漏洞」。[4]GDPR第33條[5]及第34條[6]則規定「於特定情況下，個人資料侵害事件必須向具管轄權之國家監管機關通報，並將該個人資料侵害事件通知其個人資料受到影響之當事人」。

GDPR說明個人資料侵害可能造成之影響包括：當事人喪失對其個人資料之控制權、其權利受到限制、歧視、身分冒用或詐欺、財務損失、假名化遭到未經授權之還原、名譽損害，以及受到職業保密義務保護的個人資料之機密性遭破壞，亦包含該等當事人在經濟或社會方面所遭受的任何其他重大不利益。[7]

(三)　案例式探討之必要性：

由於控管者最重要的義務之一，即為評估當事人之權利及自由所面臨的風險，並實施適當之技術上及組織上措施來緩解該等風險。透過類型化不同個人資料洩漏之案例類型，並透過評估各案例中存有之不同要素，將可以辨識各案例的風險，並評估應採取之行動。

雖然事故通報指引之案例均屬虛構，但其均係基於監管機關在個人資料侵害事件通報方面所累積的共同經驗所提出的典型案例。[8]事故通報指引中的分析雖是針對案件具體事實所為，但其目的係在協助控管者就其所涉個人資料侵害事件進行評估，俾利日後遭遇其他未列舉之個人資料侵害事件時，各國主管機關亦得本於指引文件

[4] GDPR art 4.12: 'personal data breach' means 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…

[5] GDPR art 33.1: 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.

[6] GDPR art 34.1: 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.

[7] EDPB, *supra* note 1, at 6.

[8] EDPB, *supra* note 1, at 7.

案例中說明之風險評估原則，對於該個人資料侵害事件做出最適宜的因應措施。[9]

事故通報指引所述案例之具體事實若有任何變更，均可能導致其風險程度有所變化或上升，從而需要採取不同或額外之措施，故其主要目的在於說明應如何判斷風險等級，而非可作為案例法援引。[10]處理不同類型的個人資料侵害事件時，可能需採取不同的緩解措施，但處理同一類型的個人資料侵害事件時，由於具體個案中可能有其他影響因子，因此，並不必然需採取相同之緩解措施，[11]主管機關就具體個案仍應權衡應採取的因應措施。

二、相關案例與因應方式：

(一) 勒索軟體攻擊

於勒索軟體攻擊事件中，攻擊者以惡意程式碼對個人資料進行加密，隨後要求控管者支付贖金以換取解密代碼。該等事件一般可被歸類為「可用性」侵害事件，但經常也可能屬「機密性」侵害事件。[12]以下針對不同類型予以區分。

1. 有備份且未外洩

於本案例中，攻擊者已取得經加密之個人資料，並破壞其中包含該等個人資料之密文（cipher text）的機密性。然而，攻擊者無法讀取或使用該等個人資料。因此，自然人之權利及自由所面臨的機密性風險很低，除非密碼破解技術未來有所演進，使攻擊者得以讀取加密資料。[13]於本案例中，當事人之權利及自由所面臨的風險似乎起因於個人資料喪失可用性，而個人資料之機密性並未受到影響。

[9] EDPB, *supra* note 1, at 7.
[10] EDPB, *supra* note 1, at 7.
[11] EDPB, *supra* note 1, at 7.
[12] EDPB, *supra* note 1, at 8.
[13] EDPB, *supra* note 1, at 8.

故僅需備置內部紀錄，無須通報監管機關或通知當事人。[14]

2. 未妥善備份且未外洩

於本案例中，勒索軟體對個人資料進行加密，但無法擷取資料。因此，當事人之權利及自由所面臨的風險似乎起因於個人資料喪失可用性，而個人資料之機密性並未受到影響。在識別風險時，必須對防火牆日誌及其相關意涵進行徹底研析。控管者應依據監管機關要求提出該等調查所發現之事實及結果。[15]

控管者必須瞭解，若攻擊者能力強大，惡意軟體可能會有編輯日誌檔案及刪除紀錄的功能。因此，若日誌檔案並未被傳輸或複製至中央日誌伺服器，即使經過徹底調查認定個人資料並未遭攻擊者破解，控管者也無法依據日誌檔案證明資料未遭外洩，進而無法完全排除此事件屬「機密性」侵害事件的可能性。[16]

除了資料喪失可用性可能對當事人造成影響外，缺乏備份資料庫也會被認為是提高風險程度的因素之一。除非有其他資料來源（例如：確認訂單之電子郵件），控管者若無備份資料，只能採取相當有限的措施來彌補個人資料之滅失，且相關資料均須重新蒐集。[17]若無備份，資料可能會就此滅失，而此事件的重大程度取決於對當事人所造成的影響。本案例中的勒索軟體攻擊事件，對當事人的權利及自由會造成風險，但尚未達高風險的程度。故僅需備置內部紀錄、通報監管機關而無須通知當事人。[18]

3. 醫療院所案例

醫療院所一般都會運用大量資料，因此倘遭攻擊受影響資料及受影響當事人的數量均很高。資料一旦無法使用就會對大量當事人

[14] EDPB, *supra* note 1, at 9-10.
[15] EDPB, *supra* note 1, at 10.
[16] EDPB, *supra* note 1, at 10.
[17] EDPB, *supra* note 1, at 11.
[18] EDPB, *supra* note 1, at 11.

造成重大影響。此外，病患資料之機密性也會持續遭受重大風險。[19]侵害事件之類型及受影響個人資料之性質、敏感性及數量都是很重要的因素。即使有備份資料，且能夠在數日內還原資料，但遭到攻擊後數日內喪失資料可用性，仍會使當事人受到重大影響，因此屬高風險。[20]

因為涉及特種個人資料，且還原資料可能需要很長時間，因而導致病患照護發生重大延誤，因此必須通報監管機關。由於事件會使病患受到影響，即使在還原加密資料後，仍有必要通知當事人。控管者應該直接向該等病患通知個人資料侵害事件之情況。[21]故於此案例情形下，需備置內部紀錄、通報監管機關並通知當事人。

4. 未備份且有洩漏

攻擊者可能已變更及/或複製伺服器上之資料，因此不僅涉及資料可用性，亦涉及機密性，因此，此類型侵害事件會導致高風險。因為可能會導致財物（例如：因信用卡資訊受影響而造成的財務損失）及非財物損害（例如：因身分證資訊受影響而造成之身分冒用或詐欺），[22]故於此案例情形下，需備置內部紀錄、通報監管機關並通知當事人，以利當事人得以採取必要措施來避免財物損失（例如：通知銀行止付信用卡）。[23]

(二) 個人資料外洩攻擊

此等攻擊可能與勒索軟體攻擊類似，因為風險來自於未經授權第三方之行動，但一般係為複製、擷取及濫用個人資料以達到特定惡意目的。因此，此等攻擊主要屬於「機密性」侵害事件，但亦可能屬「完整性」侵害事件。另外，若控管者瞭解此等個人資料侵害

[19] EDPB, *supra* note 1, at 12.
[20] EDPB, *supra* note 1, at 12.
[21] EDPB, *supra* note 1, at 12.
[22] EDPB, *supra* note 1, at 14.
[23] EDPB, *supra* note 1, at 14.

事件之特點，即可採取多項措施以大幅降低遭攻擊的風險。[24]

1. 網站的求職者個人資料外洩

控管者之環境安全非常重要，因為此類型漏洞多數均可透過持續更新系統、加密敏感性資料，採用高資安標準（例如：高強度驗證機制、防止暴力攻擊之措施、「轉義（escaping）」或「淨化（sanitising）」使用者輸入資訊等）進行應用程式開發以有效防範；另外亦須定期進行資訊科技安全稽核、漏洞評估及滲透測試，俾提前發現該等類型之漏洞並加以修復。[25]

控管者應持續透過識別攻擊類型及方法，展開個人資料侵害事件之調查，以評估該採取哪些措施。為確保調查快速、有效，控管者應備置事故應變計畫，於其中載明應立即採取之必要措施，以控管事故後續。[26]攻擊者不僅會破壞資料之機密性，亦會就系統進行變更，所以資料之完整性也會受到影響。[27]

基於上述，因個人資料侵害事件可能使自然人之權利及自由面臨高風險，控管者必須備置內部紀錄，並將個人資料侵害事件通知當事人，亦必須通報相關監管機關。[28]

2. 網站已雜湊的密碼外洩

於本案例中，個人資料機密性受到損害，但因資料庫中的密碼係透過最新技術進行雜湊，個人資料相關風險在性質、敏感程度及數量方面均有所緩解。於本案例中，當事人之權利及自由並未遭受任何風險。此外，當事人的聯絡資訊（例如電子郵件地址、電話號碼等）並未遭竊，這表示當事人不會面臨成為詐騙對象（例如收到網路釣魚（phishing）電子郵件或詐騙簡訊及電話等）的顯著風險。

[24] EDPB, *supra* note 1, at 15.
[25] EDPB, *supra* note 1, at 15-16.
[26] EDPB, *supra* note 1, at 16.
[27] EDPB, *supra* note 1, at 16.
[28] EDPB, *supra* note 1, at 16.

[29]

在特定情況下，向當事人發送通知得被視為緩解措施，當事人接獲通知後將得採取必要措施（例如變更密碼等）以避免因該個人資料侵害事件遭受進一步損害。惟於本案例中，控管者並不具通知義務。僅在某些情況下，發送通知會被視為適當作法。本案應僅需備置內部紀錄，無須通報監管機關或通知當事人。[30]

3. 銀行網站的憑證填充攻擊

若控管者處理的個人資料具有高度重要性，在確保資料安全方面就負有較大責任。[31]此個人資料侵害事件涉及身分及使用者帳號資訊以外之金融資料，因此影響特別重大，受影響人數眾多。在此敏感環境中會發生個人資料侵害事件，顯示出控管者的系統存在重大的資料安全性漏洞，且必須檢視及更新受影響之措施。[32]

受影響的資料使攻擊者可單獨識別當事人身分，且其中包含當事人之其他資訊（包括性別、出生日期及地點）；此外，攻擊者亦可利用該等資料猜測銀行客戶密碼或針對銀行客戶進行魚叉式網路釣魚（spear phishing）詐騙。[33]基於上述原因，此個人資料侵害事件被認為會使所有相關當事人之權利及自由面臨高風險，因此可能發生財物（如財務損失）及非財物損害（如身分冒用或詐欺）。故於此案例情形下，需備置內部紀錄、通報監管機關並通知當事人。[34]

(三) 內部人員風險源

個人資料侵害事件中必須特別注意人為錯誤所扮演的角色，因為人為錯誤很常見。由於該等類型之個人資料侵害事件有可能是蓄

[29] EDPB, *supra* note 1, at 17.
[30] EDPB, *supra* note 1, at 17.
[31] EDPB, *supra* note 1, at 18.
[32] EDPB, *supra* note 1, at 18.
[33] EDPB, *supra* note 1, at 18.
[34] EDPB, *supra* note 1, at 19.

意也可能是無心造成，控管者很難識別漏洞並採取措施避免該等漏洞。[35]

1. 員工外洩業務資料

於本案例中，公司並未採取措施防止員工複製公司客戶之聯絡資訊，因為該員工需要且確實有合法存取該等資訊來履行職務。而且在執行大多數客戶關係工作時，員工需要存取特定個人資料，該等個人資料侵害事件可能是最難預防的類型。針對存取範圍進行限制可能使員工履行職務受到限制。然而，完善的存取權限政策及持續的控管，可以協助防止該等個人資料侵害事件的發生。[36]

於風險評估過程中，應考量個人資料侵害事件的類型及受影響個人資料之性質、敏感性及數量。由於資料庫的完整性沒有受到影響，只有內容遭到複製及利用，因此此類事件一般屬機密性之侵害事件。受影響之資料數量一般屬低、中程度。於本案例中，沒有特種個人資料受到影響，該員工取得客戶聯絡資訊係為供其離職後聯繫之用，因此受影響資料並非敏感性資料。[37]

於本案例中，很難緩解個人資料侵害事件之不利影響，可能需要立即採取法律行動來防止前員工進一步濫用及傳播資料，下一步則應以避免未來發生類似事件為目標。控管者可以嘗試要求前員工停止使用資料，但此要求的成功可能性不高。採取適當的技術上措施（例如：禁止複製或下載資料至行動裝置）可能有幫助。[38]總歸而言，由於此個人資料侵害事件不會對自然人之權利及自由造成高風險，僅須備置內部紀錄並通報監管機關，無須通知當事人。[39]

2. 意外將資料傳輸至可信任的第三方

[35] EDPB, *supra* note 1, at 20.
[36] EDPB, *supra* note 1, at 20.
[37] EDPB, *supra* note 1, at 20.
[38] EDPB, *supra* note 1, at 21.
[39] EDPB, *supra* note 1, at 21.

個人資料侵害事件並非始自員工的故意行為，係因不注意而造成的非故意人為錯誤。這類個人資料侵害事件可以透過以下方式避免或降低頻率：(1)實施訓練、教育及宣導計畫，讓員工更深入瞭解個人資料保護的重要性；(2)減少透過電子郵件交換文件，改採專用系統來運用客戶資料；(3)在傳送郵件前再次檢查文件；(4)區隔創建文件及傳送文件的作業。[40]

此個人資料侵害事件僅涉及資料之機密性，完整性及可同性均未受到影響，且只有二十幾名客戶受到影響，因此，受影響的資料量很低。此外，受影響之個人資料不包含任何敏感性資料。[41]因受影響之當事人較少，且立即發現並採取措施將其影響降至最低，綜合該等因素使本案風險程度極低。[42]故此事件僅需備置內部紀錄，無須通報監管機關與通知當事人。

(四)　裝置或紙本的遺失或被竊

可攜帶式裝置之滅失或遭竊屬常見的個人資料侵害事件類型。於該等情況下，控管者必須考量到資料運用作業的相關情況（例如：儲存在該裝置上之資料類型）及輔助資源，以及於個人資料侵害事件發生前已採取的措施，以確保適當之安全水準。這些因素均會造成個人資料侵害事件之潛在影響。但因為裝置已不存在，風險評估可能很難執行。[43]該等類型之個人資料侵害事件均可被歸類為機密性侵害事件。然而，若遭竊之資料庫沒有備份，則亦屬可用性及完整性之侵害事件。[44]

1. 存放已加密個人資料之裝置被竊取

於本案例中，控管者採取充分措施，透過將裝置進行加密、部署適當的密碼保護，並就平板電腦中儲存的資料進行備份，以防止

[40] EDPB, *supra* note 1, at 22.
[41] EDPB, *supra* note 1, at 22.
[42] EDPB, *supra* note 1, at 22.
[43] EDPB, *supra* note 1, at 23.
[44] EDPB, *supra* note 1, at 24.

及緩解潛在個人資料侵害事件之影響。[45]在發現個人資料侵害事件後，控管者應評估風險來源、支援資料運用之系統、涉及之個人資料類型及個人資料侵害事件對相關個人的潛在影響。上述個人資料侵害事件會涉及相關資料之機密性、可用性及完整性，但由於控管者在個人資料侵害事件發生之前及之後均採取適當程序，相關資料之機密性、可用性及完整性均未遭到影響。[46]

由於平板電腦及應用程式均有高強度密碼保護，裝置上個人資料之機密性並未受到影響。該等平板電腦的設置方式，是在設置密碼的同時也就資料進行加密。控管者試圖透過遠端操作刪除遭竊設備上的所有資料，亦進一步提升了安全性。[47]此個人資料侵害事件不太可能對當事人之權利及自由造成風險，因此毋須通報監管機關或通知相關當事人，僅須備置內部紀錄即可。

2. 存放未加密個人資料之裝置被竊取

控管者事前並未採取任何安全措施，因此儲存在遭竊筆電中的個人資料很容易遭竊賊或後續取得該裝置的任何其他人存取。此個人資料侵害事件會影響遭竊設備上所儲存資料之機密性。[48]於本案例中，存有個人資料的筆電相當脆弱，因為其不具備任何密碼保護或加密功能。缺乏基本安全措施提高了受影響當事人之風險程度。此外，因無法識別當事人，也提升了此個人資料侵害事件的重大性。[49]

受影響人數眾多也提高了風險；雖然如此，此個人資料侵害事件並未涉及種個人資料。控管者應考量機密性遭侵害的潛在後果及不利影響。由於發生此個人資料侵害事件，相關當事人可能會因為遭竊裝置上的資料而遭受身分詐欺，所以此事件被認為屬高風險。

---

45 EDPB, *supra* note 1, at 24.
46 EDPB, *supra* note 1, at 24.
47 EDPB, *supra* note 1, at 24.
48 EDPB, *supra* note 1, at 25.
49 EDPB, *supra* note 1, at 25.

[50]於上述情況，有必要備置內部紀錄、通報監管機關，也必須通知相關當事人。

3. 被竊取的紙本文件有敏感性資料

控管者事前並未採取任何安全措施，因此儲存在此紀錄本中的個人資料很容易被持有此文件者存取。此外，有鑑於本文件中個人資料之性質，使得缺乏備份資料成為非常重大的風險因素。本案為高風險個人資料侵害事件案例。由於未採取適當的安全預防措施，GDPR第9.1條所載之敏感健康資料因此滅失。[51]

由於本案涉及特種個人資料，相關當事人之潛在風險增加，這也是控管者於評估風險時所必須考量的因素。此個人資料侵害事件涉及影響相關個人資料之機密性、可用性及完整性。[52]由於此個人資料侵害事件，醫療機密性會受到侵害，未經授權之第三方可能取得病患的私人醫療資訊，這可能對病患的個人生活造成重大影響。此個人資料侵害事件可能會對相關當事人造成重大影響，因此必須將此個人資料侵害事件備置內部紀錄、通報監管機關並通知相關當事人。[53]

(五) 郵遞錯誤

風險來源同樣是內部人為錯誤，但個人資料侵害事件並非是惡意行動所造成，而是不注意的結果。於事件發生後，控管者能夠採取的措施很少，因此於此等情況下，採取預防措施比其他類型事項更加重要。[54]

1. 誤寄包裹

裝箱單中記載成功送貨所必須的個人資料（姓名、地址、購買

[50] EDPB, *supra* note 1, at 25.
[51] EDPB, *supra* note 1, at 26.
[52] EDPB, *supra* note 1, at 26.
[53] EDPB, *supra* note 1, at 26.
[54] EDPB, *supra* note 1, at 27.

商品及其價格）。首要任務是判斷人為錯誤是如何發生，以及是否得以任何方式防止該錯誤。本案例所涉風險很低，因為不涉及特種個人資料，亦不涉及其他一旦遭濫用就可能導致重大不利影響的資料；[55]此個人資料侵害事件並非係因控管者之系統錯誤所造成，且僅涉及兩個人，並未對該等個人造成不利影響。因個人資料侵害事件本身並不會對受影響個人之權利及自由構成高風險，控管者僅需備置內部紀錄，無須通報監管機關或通知當事人。[56]

2. 誤寄極機密個人資料

針對該等訊息之發送原即應考量採取額外的控管機制以實施更嚴格的規範。本案例因受影響個人數量眾多，並涉及其社會安全號碼及其他更基本的個人資料，因此進一步提高風險；本事件因此可確認屬高風險。[57]有效緩解此類事件風險的措施相當有限，雖然控管者要求刪除資訊，但無法強迫收件人遵守，因此無法確定收件人是否確實遵守該要求。故應備置內部紀錄，並應通報監管機關及通知當事人。[58]

3. 誤寄個人資料

原本即應考量採取額外的控管機制，針對該等含有個人資料訊息之發送實施更嚴格的規範。本案例所涉依據該等個人資料之性質、敏感性、數量及脈絡判斷，此事件之風險很低。遭揭露之資料數量及受影響當事人之數量亦非常少。[59]控管者於發現錯誤後立即與收件人聯絡，這一事實可以被認為是緩解影響的因素。基於上述，此個人資料侵害事件不太可能對當事人之權利及自由造成風險，因此毋須通報監管機關或通知相關當事人，僅需備置內部紀錄即可。[60]

---

55 EDPB, *supra* note 1, at 27.
56 EDPB, *supra* note 1, at 27.
57 EDPB, *supra* note 1, at 28.
58 EDPB, *supra* note 1, at 28.
59 EDPB, *supra* note 1, at 29.
60 EDPB, *supra* note 1, at 29.

4. 全自動發送保費繳款單

自動發送之錯誤信件內含姓名、地址、出生日期、未遮蔽之車輛牌照號碼及本年度及下一年度之保險費率分類。當事人所受影響程度被認為屬中等，因為非公開資訊（如出生日期或未遮蔽之車輛牌照號碼，及關於保險費率增加之詳細資訊）遭揭露予未經授權之收件人。該等資料遭到濫用的機率被評估為於低等及中等之間。[61] 控管者應自費退還原始文件，亦應告知錯誤的收件人不得濫用其因此取得之資訊。本案件建議備置內部紀錄並通報監管機關，而無須通知當事人。[62]

(六) 其他案例—社交工程

1. 身分冒用

此案例說明採取事前防範措施的重要性。從風險方面來看，此個人資料侵害事件涉及高度風險，因帳單資料涉及當事人之私人生活資訊（例如：習慣、聯絡人），並可能導致財物損失（例如：遭跟蹤，對人身完整性造成風險）。於此等事件中取得的個人資料亦得被用來接管該帳戶或利用該公司所設置的其他認證措施。考量到該等風險，實施「適當」認證措施的標準相當高，並取決於通過認證後可利用的個人資料範圍。[63]因此，除備置內部紀錄外，控管者必須通報監管機關亦應通知當事人。[64]

2. 電子郵件外洩

即使攻擊者很可能並非以蒐集個人資料為目的，但由於資訊揭露可能導致財物(如財務損失)及非財物損失(如身分冒用或詐欺)，或資料可能被用於從事其他攻擊（如網路釣魚），此個人資料侵害

[61] EDPB, *supra* note 1, at 29-30.
[62] EDPB, *supra* note 1, at 30.
[63] EDPB, *supra* note 1, at 31.
[64] EDPB, *supra* note 1, at 31.

事件可能對自然人之權利及自由造成高風險。[65]因此，除備置內部紀錄外，控管者必須通報監管機關亦應通知當事人。[66]

第三節 與我國個人資料保護法之重點比較

一、 我國個人資料保護法針對個人資料侵害事件之規範

我國個人資料保護法有關個人資料侵害事件通知當事人規定於第12條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」，通知當事人之方式規定於個人資料保護法施行細則第22條。而個人資料保護法第18條、第27條及個人資料保護法施行細則第12條則概括性地要求公務機關與非公務機關應辦理安全維護事項或採行適當之安全措施以防止個人資料侵害事件之發生。是以，現行個人資料保護法未明文規定公務機關及非公務機關對於個人資料侵害事件通報主管機關之義務。

相對的，有關將個人資料侵害事件通報主管機關一事，我國法多係訂於各中央目的事業主管機關訂定之個人資料檔案安全維護管理辦法，於其中要求業者應訂定應變、通報及預防機制，最常見者包含：事故發生後應採取之應變措施，包括降低、控制當事人損害之方式、查明事故後通知當事人之適當方式及內容；業者遇有消費者個人資料安全事故，應於知悉事故後七十二小時內通知主管機關。

然而，我國各主管機關所訂定之辦法並未進一步就不同案件類型與風險等級進行分類，亦無明文規定各類型案件之處理方式，或對於個人資料侵害事件帶來影響的緩解措施。此外，針對是否通知監管機關，我國多數主管機關係以有無危及正常營運或大量當事人權益進行判斷，但對於何謂大量當事人權益卻無明確定義。部分個

[65] EDPB, *supra* note 1, at 32.
[66] EDPB, *supra* note 1, at 32.

人資料檔案安全維護管理辦法雖嘗試量化，例如內政部指定警政類非公務機關個人資料檔案安全維護管理辦法[67]以及宗教團體個人資料檔案安全維護管理辦法[68]，其規定非公務機關遇有達五千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關，似乎係以五千筆以上個人資料事故作為區分有無通報必要的標準，但此標準應僅限於適用此規定之行業別，其餘業者對於大量當事人權益之認定並不受此規定之拘束。

從我國對於個人資料侵害案件之上述規範，可以發現我國欠缺一個較有體系的法律架構以處理個人資料侵害案件。以下本文將從GDPR及事故通報指引的規範方式，探討我國法較需進一步調整之處。

二、 GDPR、指引文件與我國法之不同

(一) 被要求負有通報義務之主體

由於個人資料保護法並未直接要求業者須通報主管機關，故僅有中央目的事業主管機關有訂定個人資料檔案安全維護管理辦法，且該辦法有規定需要負擔通報主管機關義務之行業，始負有通報義務。有鑑於並非所有行業別的中央目的事業主管機關均有訂定個人資料檔案安全維護管理辦法，故並非所有業者遇到個人資料侵害事件時均有通報主管機關之義務。

再者，縱使中央目的事業主管機關有訂定個人資料檔案安全維

[67] 內政部指定警政類非公務機關個人資料檔案安全維護管理辦法第 8 條第 2 項：「非公務機關遇有達五千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報主事務所所在地之直轄市、縣（市）主管機關，並副知中央主管機關……」

[68] 內政部指定宗教團體個人資料檔案安全維護管理辦法第 8 條第 2 項：「宗教團體遇有達五千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報其主管機關。如為直轄市、縣（市）主管機關接獲通報，並應副知中央主管機關……」

護管理辦法，亦非所有經營該行業別之業者均適用該管理辦法之規定。舉例言之，製造業及技術服務業個人資料檔案安全維護管理辦法第2條第1項即規定保有消費者個人資料未達五千筆之業者，不需要受到該管理辦法的規範，從而亦無需遵守相關個人資料侵害事件的通報、報告義務。[69]

相對的，在歐盟的規範下，GDPR及事故通報指引均未特別依照行業別而區分適用。是以，無論經營何種行業，或保有消費者多少個人資料筆數，均受到相關個人資料侵害事件應盡義務之規範。固然有論者可能認為對於部分小型業者抑或是僅存有非敏感性個人資料之業者，此規範模式過於嚴苛，惟在歐盟法的規範邏輯下，因應措施是透過風險評估進行判斷，自事故通報指引當中即可知悉，對於業者保有的個人資料筆數較低且機密性、敏感性同樣較低時，相關需要進行的緩解措施也同樣會給予較輕微的義務要求，並不會因為將該些業者納入規範對象，而令其負有不相當的義務。

反之，若是自始即不將該些業者納入規範對象，即有可能錯誤評估風險，倘若此類未被納管的業者發生較為嚴重的個人資料侵害案件時，反而缺乏法源依據要求其負有通報、緩解等義務。因此，對於當事人的權益保障而言，應採取歐盟法的規範模式較為妥適。

(二) 通知之要件與風險評估之標準

在通知對象的設計上，我國個人資料檔案安全維護管理辦法與歐盟法的規範大致相同，同樣要求通知當事人以及通報主管機關，然而，在判斷需否進行通報的標準上，我國法則與歐盟法相差甚遠。

由於我國法是透過不同目的事業主管機關訂定個人資料檔案安全維護管理辦法進行規範，如此將造成在判斷應否通報主管機關

[69] 製造業及技術服務業個人資料檔案安全維護管理辦法第 2 條第 1 項：「保有消費者個人資料之製造業及技術服務業業者（以下簡稱業者），應依本辦法規定，規劃、訂定、修正與執行消費者個人資料檔案安全維護計畫（以下簡稱本計畫）。但保有消費者個人資料未達五千筆之業者，不在此限。」

的要件上產生諸多歧異。相關規範的模式大致可分為三類：

1. 有如中藥批發零售業個人資料檔案安全維護計畫實施辦法並未特別規定要件，僅須於查明事故發生原因及損害狀況，即應於發現事故時起七十二小時內，通知當事人或其法定代理人，並通報直轄市、縣（市）主管機關及通知中央主管機關者；[70]

2. 有如製造業及技術服務業個人資料檔案安全維護管理辦法，查明事故後通知當事人，而在業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益時，始應於知悉事故後七十二小時內通報主管機關者；[71]

3. 有如內政部指定警政類非公務機關個人資料檔案安全維護管理辦法，查明個人資料事故後通知當事人，並於遇有達五千筆以上之個人資料事故時，於發現後七十二小時內將通報主管機關者。[72]

上述通報要求的不同並無法從規範的行業別差異中整理出區分的實益與邏輯，故明顯僅係不同主管機關間在規範設計上並未達成共識的結果。如此將會造成對於應通報事件認定上的不一致，並

[70] 中藥批發零售業個人資料檔案安全維護計畫實施辦法第 14 條第 1 項：「中藥批發零售業者，訂定第四條第四款事故之預防、通報及應變機制，應包括下列事項：
一、採取適當措施，控制事故對當事人造成之損害。
二、查明事故發生原因及損害狀況，並於發現事故時起七十二小時內，以適當方式通知當事人或其法定代理人，並通報直轄市、縣（市）主管機關及通知中央主管機關；未於時限通報者，應附記理由。
三、研議改進措施，避免事故再度發生。」

[71] 製造業及技術服務業個人資料檔案安全維護管理辦法第 6 條第 2 項：「業者遇有消費者個人資料安全事故，將危及其正常營運或大量當事人權益者，應於知悉事故後七十二小時內依附表二格式通報經濟部（以下簡稱本部），或通報直轄市、縣（市）政府時副知本部。」

[72] 內政部指定警政類非公務機關個人資料檔案安全維護管理辦法第 8 條第 2 項：「非公務機關遇有達五千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報主事務所所在地之直轄市、縣（市）主管機關，並副知中央主管機關……」

無法確實依照個人資料侵害事件的風險等級反映出需採行的通報措施。

而在歐盟的規範上則明顯與我國採取不同方式，依照事故通報指引的規範，應採行個人資料侵害事件應對措施均係基於該事件的風險等級不同，而設計控管者應當負擔的責任。又因為歐盟十分強調依風險訂定應採行之措施，故在GDPR此類根本性規範下，並不適合逕行訂定較為細節性的規定，而是先以框架性規範訂於GDPR中，再透過如事故通報指引的模式，進行補充。在事故通報指引中，雖然有依照諸多不同類型區分應採取的措施，但是觀察每一個案例中所納入考量的要素，其實是有其一致性的。舉例言之，資料的筆數、資料的類型、有無加密等要素均一再被納入評估該個人資料侵害事件的風險等級中。

再者，在採用相類似的判斷標準時，歐盟之規範方式同樣更能貼近風險的程度予以因應。如我國雖然同樣有部分主管機關對於是否應通報採用資料的筆數進行區分，然而，其我國規範上係單純以五千筆作為分野，透過一個既定的個數作為認定將造成僵化認定的結果，在此種規範方式下，可能造成未達五千筆則無論個人資料的類型以及洩漏的情狀，均無須通報主管機關的法律效果。試想，若兩千筆個人資料均係敏感性個人資料，其被洩漏之情形似乎仍然應被認定為重大，而需要採取較高程度的措施。是以，此種認定模式較不妥適。

至於我國部分主管機關透過概括性法律概念進行規範的模式，確實較具有彈性，惟該些主管機關並未公開其認定重大侵害當事人權益的標準，將會令業者無從遵循，並且造成法律之不可預見性。我國主管機關實應採取如事故通報指引的方式，通過公開其對於不同案例上的認定標準，並且告知各該業者其主要會參採的要素，以進一步明確化何謂重大侵害當事人權益而需要通報主管機關。如此應可提高在發生個人資料侵害事件時，業者遵循法律規範的可預見

性。

最後，由於個人資料保護法第12條並未就通知當事人的義務設定任何門檻或條件，觀察我國主管機關目前訂定之個人資料檔案安全維護辦法，可以發現個人資料侵害事件時的通知義務上，我國主管機關多會認為需要通知當事人。相對的，對於應通知主管機關的情形，卻設有許多限制。此部分的概念同樣與事故通報指引的規範有所不同。在事故通報指引中，最基本的處理措施有三者：備置內部紀錄、通知監管機關、通知當事人，其中通知當事人的情形通常須為該個人資料侵害事件的風險係數較高時始產生。

在此規範差異上，本文以為由於通知當事人將會造成當事人對於控管者較大的疑慮，且對於控管者而言，通知當事人的成本亦較高（倘若受侵害之個人資料筆數較多時）。是以，通知當事人之義務應適用於個人資料侵害風險等級較高的情形。而在主管機關的通報上，由於僅須向具有監管權能的主管機關報告，成本上較低，且如果此資料並非法律規定主管機關應向民眾公告者，對於業者的商譽影響亦較低，是以，通報主管機關應可視為一個較低程度的義務。且主管機關本即更需掌握業者對於個人資料的保護程度以及相關發生的風險情形，故與通知當事人相較，通報主管機關理論上不應作為發生較嚴重個人資料侵害事件時始需進行的行為。

自此可知，歐盟在事故通報指引當中的設計較為符合個人資料侵害事件風險等級的認定，也同時符合防護個人資料侵害事件的設計，我國對於通知義務的規定建議可參酌調整。

第四節 小結

綜上所述，我國目前對於個人資料侵害事件的規範有諸多未竟之處，現行規範設計無法確實反應個人資料侵害事件的風險等級，透過將各該緩解措施訂於不同目的事業主管機關所設計的個人資料檔案安全維護辦法中，亦可能造成部分行業別或是一定規模以下的業者成為漏未受規範

者，如此將可能造成當事人暴露於個人資料受到侵害的風險中。

是以，本文參考GDPR以及事故通報指引的規範設計架構，認為我國實應參酌歐盟法的規範模式，多考量可能影響個人資料侵害事件風險的要素，並不採用僵化性的區分標準，以達到正確反應風險等級而採取因應措施的效果。而在法規調適上，若我國設置個資保護獨立監督機制後，建議以下幾個修正方向：

一、 修改個人資料保護法，將通報義務等調適措施透過概括性的法律概念施以規範，以避免有行業別漏未受到此通報義務的要求。

二、 透過類似於事故通報指引的規範方式，以案例介紹之方式，令相關業者與各目的事業者主管機關了解面對個人資料侵害事件時應考量的判斷因素，以及對於較為常見的案件類型建議處理之方式。然由於案例式的建議內容過於龐雜，可能不適合直接訂於法令中，又為確保日後遭遇新型態的攻擊時，亦能具有快速因應的彈性，因此可能同樣建議採取指引、行政指導的模式，以針對不同型態的個人資料外洩建立處理程序與機制。

三、 由統一之中央主管機關發布類似事故通報指引，始可避免不同目的事業主管機關間可能產生之規範歧異。畢竟，針對個人資料侵害事件，並無必要依行業別而區分適用，可以透過在依照風險因子判斷風險等級時處理。中央主管機關於訂定規範內容時，亦不應比照目前個人資料檔案安全維護管理辦法中較僵化或不明確的規範模式，建議參酌歐盟法以風險等級為基礎的設計方式為之。

四、 於確立相關機制建構後，應可將現行於各目的事業主管機關訂定的個人資料檔案安全維護管理辦法中，刪除現有與個人資料侵害事件相關的通知義務、處理措施，以統一個人資料侵害或外洩事件的處理程序。

倘我國得依照上述建議嘗試調整現行的規範架構，本文以為對於我國業者在遵循相關處理原則與規範上將會更具有明確性，並可同時加強

對於當事人的權益保障，建構一個更完善且健全的個人資料保護制度。

第二章 GDPR控管者與受託運用者概念指引（Guidelines 07/2020）[73]

第一節 簡介

於解釋適用GDPR規定時，「控管者（controller）」、「受託運用者（processor）」以及「共同控管者（joint controller）」三者概念之區辨甚為重要。這幾個概念涉及不同主體於GDPR規定、個人資料保護法律下所負擔義務、以及當事人如何行使權利。此外，GDPR第5條要求資料之完整性與保密性，即控管者應對第5條中與運用個人資料之事項負責並應採取適切之技術性及組織性安全措施，以證明資料之處理符合GDPR規範。

抑有進者，GDPR引入更具體的受託運用者相關規範，並且針對控管者與受託運用者訂定個人資料運用之規定。為確保上述概念之解釋標準於歐洲經濟區（EEA）中清楚一致[74]，EDPB於2021年7月7日通過（復於2022年9月20日微幅修訂）「GDPR控管者與受託運用者概念指引」（下稱「控管者與受託運用者概念指引」），旨在釐清GDPR下控管者、受託運用者與共同控管者之定義、控管與受託運用者法律關係、共同控管關係、責任歸屬分配、以及當事人得以如何主張權利。[75]

控管者與受託運用者概念指引主要分為兩部分，第一部分討論控管者、共同控管者、受託運用者和第三方／資料接收方等不同概念的定義；而第二部分就控管者、共同控管者和受託運用者不同角色間關聯與責任分擔提供進一步指引。本文將於以下「第二節 內容摘要」中進一步闡述與說明。

第二節 內容摘要

一、 GDPR定義

於GDPR架構下，區別「控管者」與「受託運用者」之實益在於GDPR

[73] EDPB, '*GUIDELINES 07/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR*', 20 September 2022 (Version 2.1).
[74] EDPB, *supra* note 73, at 7-8.
[75] EDPB, *supra* note 73, at 3.

之完整性和保密性義務。依據GDPR第5.1(f)條規定，「個人資料之處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理並防止意外遺失、破壞或損壞。」[76]此外，依據GDPR第5.2條，控管者應遵守資料完整性與保密性等義務並負舉證責任。[77]換言之，於GDPR架構下，控管者與受託運用者將遵守不同的資料保護規則，且控管者就資料整體完整與保密性保護措施之實行負擔舉證義務，因之，清楚辨別相關角色的定義即有重要之區別實益。

(一) 控管者（Controller）

原則上，可做為控管者之主體並未受限，然而於實務上控管者多為「組織」本身，而非組織內之個人（例如，執行長、員工或董事會成員）。控管者對於個人資料之運用相當關鍵，控管者之身分可能法律界定，或依據個案事實之解釋與分析，此外，合約條款通常亦有助於識別控管者之身分（然而並非適用於所有情況）。[78]

控管者之定義依據GDPR第4.7條為「單獨或與他人共同確定運用個人資料的目的和方式的自然人或法人、公務機關、機構或其他團體；如果這類運用的目的和方式由聯盟或成員國法律確定，則控管者或其提名的具體標準可由聯盟或成員國法律規定」。[79]依據控管者與受託運用者概念指引，GDPR下控管者之要件進一步被分為五項，即：「自然人或法人、公務機關、機構或其他團體」、「決定」、「單獨或與他人共同」、「目的及方式」以及「個人資料的運用」。

[76] GDPR art 5.1(f): personal data shall be…(f) processed in a manner that ensures 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 ('integrity and confidentiality').

[77] GDPR art 5.2: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

[78] EDPB, *supra* note 73, at 3.

[79] GDPR art 4.7: '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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[80]除「共同控管者」將於下節討論，以下分述其餘要件：

控管者角色的實體類型並未受限，雖然並未排除控管者可能為個人或數名個人，然實務上控管者大多為「組織本身」，如公司或政府機構指定特定人員運用資料，該個人並非控管者，而係代表法人實體執行業務者。[81]所謂「決定」係指控管者藉由行使決策權對個人資料的運用產生影響。依據控管者與受託運用者概念指引，可被認為引起控管的情形包含(1)源於法律規定的控管；以及(2)來自事實影響的控管。其中，於認定事實影響之控管時，控管者的角色並非源於運用資料的實體本質，而應依據該實體於特定背景下的具體活動，考量相關事實以推斷。因某些運用活動可被視為與最終承擔責任的實體角色或活動當然相關聯。[82]

所謂「目的及方式」之判斷之重要性在於，「資料必須為特定、明確和合法目的而蒐集，且不得以與這些目的不相符的方式進行進一步運用。」因而，控管者並非僅決定目的，亦須決定運用的方式；換言之，受託運用者則無法決定運用資料之目的。[83]最後，就「個人資料的運用」而言，GDPR第4.2條將個人資料運用定義為「對個人資料或個人資料集執行的任何操作或一系列操作」。[84]因此，如個人資料運用過程可被劃分為數個運用操作，則得以考慮各行為人各別之目的與方式，運用資料將可能涉及一個或多個共同控管者。此外，依據控管者與受託運用者概念指引，將運用活動外包並於此過程中對運用目的及（必要）方式具有決定性影響者將被視為控管者。[85]

(二) 共同控管者（Joint Controller）

---

[80] EDPB, *supra* note 73, at 9-10.
[81] EDPB, *supra* note 73, at 10
[82] EDPB, *supra* note 73, at 11-12
[83] EDPB, *supra* note 73, at 14
[84] GDPR art 4.2: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction…
[85] EDPB, *supra* note 73, at 17.

承繼上述章節中，於控管者係「單獨或與他人共同」之要件，如有多於一位行為人之參與，則可能產生共同控管者之情形。GDPR規範共同控管者之概念，且明定各方法律關係與定義。針對上述GDPR第4.7條對於控管者之定義，GDPR第26條進一步闡述「在二個或多個控管者共同決定運用的目的及方式時，他們應為共同控管者。」[86]需構成共同控管者，應有二個以上實體「共同參與」決定運用個人資料之行動、目的以及方法。所謂「共同參與」，可能包含(1)二個以上之主體共同決定的形式；或(2)來自二個以上實體的一致決定。就該等主體共同決定，判斷重點在於(a)各參與方就該等決定彼此互補，且係運用所必需；(b)各主體對決定運用的目的和方法有實質影響；且(c)如無各方之參與，則無法進行運用。換言之，共同控管之間具有緊密之連結，且必須同時決定目的、另一方面亦決定方法。[87]共同決定的概念需要考慮的是運用的目的和方式，並非當事人間商業關係之其他面向，依據控管者與受託運用者概念指引，並非所有涉及多個實體的運用操作都會產生共同控管。存在共同控管的首要標準為二個或多個實體共同參與決定運用操作的目的和方式。[88]此外，如參與同一運用操作之實體為共同目的而運用資料時，即形成共同控管。換言之，如不同的控管者，於一系列運用中，為各自之目的運用資料，則不存在共同控管。[89]

(三) 受託運用者（Processor）

受託運用者之定義依據GDPR第4.8條為「代表控管者運用個人資料的自然人或法人、公務機關、機構或另一個團體」[90]；又依據控管者與受託運用者概念指引，受託運用者之兩項定義為：「與控管者

[86] GDPR art 26: Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers…
[87] EDPB, *supra* note 73, at 3.
[88] EDPB, *supra* note 73, at 19.
[89] EDPB, *supra* note 73, at 21-22
[90] GDPR art 4.8: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

有關的獨立實體」、以及「代表控管者運用個人資料」。[91]

依據上述統整，受託運用者為代表控管者運用個人資料的自然人或法人、公務機關、機構或其他主體。受託運用者代表控管者運用個人資料，且與控管者應為獨立之實體。區別受託運用者之實益在於，如受託運用者逾越控管者指示，並決定自身運用目的與方法，則就該運用之項目，受託運用者將可能被視為控管者。如受託運用者之行為違反GDPR，亦可能因逾越控管者指示而受罰。針對逾越控管者指示之判斷，除了非依據控管者之指示，受託運用者不得運用資料；控管者雖得於一定程度上給予受託運用者裁量空間，惟該裁量之空間不得逾越受託運用者之合適的科技上與組織上方法，並應符合控管者利益。[92]

同時，依據控管者與受託運用者概念指引，於考量是否將個人資料的運用委託給特定服務提供者時，控管者則應評估相關服務提供者是否允許他們行使足夠的控制權，同時考慮資料運用的性質、範圍、背景和目的，以及當事人的潛在風險。[93]

(四) 第三人（Third Party）或資料接收方（Recipient）

控管者與受託運用者概念指引中另定義第三人（Third Party）與資料接收方（Recipient）之概念。然而，有別於控管者及受託運用者，GDPR並未規定接收方和第三方的具體義務或責任。

依據GDPR第4.10條規定，第三方為「自然人或法人、公務機關、機構或團體；且非當事人、控管者、受託運用者和在控管者或受託運用者直接授權下運用個人資料者。」[94]依據控管者與受託運用者概念指引，第三方通常被理解為隸屬於控管者或受託運用者的法人

[91] EDPB, *supra* note 73, at 3.
[92] EDPB, *supra* note 73, at 4.
[93] EDPB, *supra* note 73, at 27.
[94] GDPR art 4.10: 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

實體者（例如：員工）。[95]

依據GDPR第4.9條規定，接收方為「定義為個人資料的揭露對象，包括自然人或法人、公務機關、機構或另一個團體，無論是否為第三方」[96]換言之，例如，當控管者將個人資料傳予另一實體（受託運用者或第三方）時，該實體即為接收方。依據控管者與受託運用者概念指引，接收資料的第三方在收到資料後，應被視為其為自身目的進行任何運用的控管者。[97]

二、 控管者與受託運用者之關係

(一) 受託運用者之選任

控管者應評估受託運用者對於GDPR遵循之風險。控管者委託的受託運用者，應保證將執行適當的技術上與組織上方法，以便以符合GDPR規範之方式運用個人資料。就此而言，控管者之考量因素可能包含受託運用者之專業知識（例如，關於安全措施與資料侵害的技術專業）、受託運用者之可靠程度、受託運用者之資源及受託運用者遵守認可的行為準則或認證機制。[98]

(二) 控管者與受託運用者之契約或其他法律文件之格式要求

依據GDPR第28.3條規定，受託運用者對於資料之處理必須受到契約或其他法律文件之控管，該等契約或法律文件必須書面（包含電子檔方式）形式為之，並且具有拘束力。此外，建議文件中包含必要的簽名以避免難以證明合約或其他法律文件之效力。[99]

(三) 控管者與受託運用者之契約或其他法律文件之內容要求

如前所述，受託運用者運用個人資料，應透過具拘束力的書面

[95] EDPB, *supra* note 73, at 29.
[96] GDPR art 4.9: 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
[97] EDPB, *supra* note 73, at 30.
[98] EDPB, *supra* note 73, at 4.
[99] EDPB, *supra* note 73, at 30-31.

（包含電子形式）合約或其他法律文件所規範。控管者和受託運用者得以選擇協商其委託合約，其可能包含所有強制規定、或全部或部分採用與GDPR第28條有關義務之標準合約條款。[100] GDPR列出委託契約應記載事項。然而，委託契約不應僅重述GDPR條文，為確保符合委託契約之目的，該契約應包含更明確和具體的內容，包括如何遵守相關規定以及個人資料運用需要何種安全層級。[101]

合約雖應涵蓋GDPR第28.3條規定之要素，然委託契約不得單純重申GDPR規範，而應依據處理者所處理之特定具體事件對其當事人權利或自由所負擔之風險做出相對應之考量。[102]依據控管者與受託運用者概念指引，GDPR第28.3條規定下，契約或其他法律文件所應闡明之項目包含：(1)受託運用者僅得處理控管者經由文件指示之資料；(2)受託運用者必須確定獲得授權運用個人資料者已承諾保密或有適當法定保密義務；(3)受託運用者必須採取一切GDPR第32條規定之措施（即：控管者應採取適切之技術性及組織性安全措施）；(4)受託運用者委託另一位受託運用者時必須遵守GDPR第28.2條及第28.4條規定的條件；及(5)受託運用者應協助控管者履行回覆當事人行使相關權利之請求；(6)終止運用活動時，依據控管者之裁量，受託運用者應刪除或將所有個人資料歸還控管者並刪除現有副本；(7)受託運用者應提供控管者足證其遵守第28條規定義務之資訊，並配合由控管者或由控管者委任之審計人員進行查核。[103]

(四) 控管者指示違反個人資料相關法令之處理

如果受託運用者認為指令違反GDPR或其他歐盟或成員國的資料保護規定，則必須立即通知控管者。而控管者必須評估狀況並查明該指令是否確實違反資料保護法。[104]

---

[100] EDPB, *supra* note 73, at 32.
[101] EDPB, *supra* note 73, at 34.
[102] EDPB, *supra* note 73, at 35.
[103] EDPB, *supra* note 73, at 36-41.
[104] EDPB, *supra* note 73, at 41.

(五) 如受託運用者決定處理之目的與方法，將被視為控管者

如前所述，一旦受託運用者決定運用的目的及方式，而違反規定，則受託運用者將被視為該運用的控管者。[105]

(六) 次受託人（Sub-processors）

鑒於運用個人資料時，隨著逐漸增多之參與者執行與運用之過程，不同層級間之委託人、受託人關係將越趨複雜。因而，就受託運用者欲委託另一人時運用個人資料時，GDPR則對此關係加諸義務。

GDPR第28.2條規定，未經控管者事先以書面特定或概括授權，受託運用者不得委託其他受託運用者。[106]換言之，控管者居於決定運用目的和方式的關鍵角色。就概括授權之情形，受託運用者應通知控管者任何其他受託運用者增加或變更之計畫，俾使控管者得以表示異議。反之，控管者亦得以事前書面授權，亦即，授權特定時間及特定運用活動有關的特定次受託人。控管者在簽署合約時決定接受某些次受託人時，經核准的次受託人名單應作為合約附件。[107]概括授權與特定授權之區分實益在於預設控管者之意思，亦即，如於概括授權之情形，如控管者未於一定期間內表達異議，將被認為同意授權。

受託運用者委託次受託人時，應簽訂契約，以課予次受託人對於第一個受託運用者所加諸之相同義務。此外，無論控管者所建議之篩選標準為何，受託運用者應為次受託人義務的履行，對控管者負全部責任。[108]

---

[105] EDPB, *supra* note 73, at 42.

[106] GDPR art 28.2: The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

[107] EDPB, *supra* note 73, at 42.

[108] EDPB, *supra* note 73, at 43.

三、 共同控管者關係

(一) 明確約定共同控管者間對於GDPR遵循之責任範疇

依據GDPR第26.1條規定，共同控管者應以透明方式確定並就各自遵守本規則義務的責任達成合意。[109]

因而，共同控管者應以透明方式確定並商定各自責任，以遵守GDPR規定之義務。[110]確定各自責任時，應考量當事人權利的行使及對其告知之義務。依據控管者與受託運用者概念指引，當事人行使GDPR所定權利時，共同控管者應界定分別由誰負責回應當事人請求，並按照GDPR第13條[111]及第14條[112]規定提供資訊給當事人。[113]

除此之外，依據控管者與受託運用者概念指引，義務並無須於共同控管人間平均分配。共同控管者對分配義務享有一定程度的彈性，共同控管者僅須確保資料運用符合GDPR規定。分配應考慮有能力並能有效確保當事人權利者，或遵守GDPR規定的相關義務等。責任分配以及法遵措施應涵蓋控管者的其他義務，其包含但不限於，關於一般資料保護原則、法律依據、安全措施、資料洩露通知義務、資料保護影響評估、受託運用者之委託、資料傳輸至第三國，以及當事人及監管機構間聯繫組織。[114]

---

[109] GDPR art 26.1: Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

[110] EDPB, *supra* note 73, at 43.

[111] GDPR art 13.1: Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information…

[112] GDPR art 14.1: Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information…

[113] EDPB, *supra* note 73, at 44.

[114] EDPB, *supra* note 73, at 44-45.

(二) 共同控管者間就責任分配必須有明確之安排

GDPR未明確規定共同控管者之間安排的法定形式。然而，為確保法律明確性、透明度及課責性，EDPB建議以具有約束力的文件進行此類安排，例如，依據歐盟或成員國法律簽訂以控管者為當事人的合約或其他具有法律約束力的文件。[115]

此外，針對上述共同控管者之間之安排，GDPR另訂有數項共同控管者對於當事人之義務，控管者與受託運用者概念指引整理如以下項目，其包含但不限於(1)安排應充分反映共同控管者各自相對於當事人的角色和關係；(2)使當事人得知悉該等安排之要素（例如當事人行使特定權利之負責人）；(3)共同控管者並得指定供當事人聯繫之窗口；此外(4)無論安排的條款如何，當事人均得行使有關反對各共同控管者的權利。[116]

除當事人外，共同控管者應規畫與監管機關溝通之方式（包含依據GDPR第36條規定之諮詢、個人資料侵害通知、資料保護長的指定等），惟監管機關則不受該等約定與安排之條款拘束，因此監管機關得聯絡任何之共同控管者，並行使其依第GDPR第58條[117]關於資料共同運用規定的職權。[118]

控管者與受託運用者概念指引並總結以上安排之重點在於，共同控管者應預先規畫回覆當事人的請求之方式，並且有效處理當事人之請求，避免當事人行使權利之負擔，而違反GDPR促進當事人行使權利的宗旨。[119]

第三節 與我國個人資料保護法之重點比較

一、我國個人資料保護法未就「控管者」概念具體定義

[115] EDPB, *supra* note 73, at 46.
[116] EDPB, *supra* note 73, at 46-48.
[117] GDPR art 58.1: Each supervisory authority shall have all of the following investigative powers…
[118] EDPB, *supra* note 73, at 47-48.
[119] EDPB, *supra* note 73, at 48.

依據個人資料保護法第4條規定:「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」；又依據個人資料保護法第2條第7款規定：「公務機關指依法行使公權力之中央或地方機關或行政法人。」個人資料保護法第2條第8款則規定:「非公務機關指前款以外之自然人、法人或其他團體。」因而，我國個人資料保護法就資料蒐集主體，區分為「公務機關」及「非公務機關」，似與歐盟有所不同。然而，有論者認為「公務機關」及「非公務機關」蒐集、處理或利用個人資料行為，應有我國個人資料保護法適用，此與GDPR「控管者」概念相當。[120]

雖然公務機關與非公務機關作為蒐集主體，可能與控管者之概念相當，惟此種立法方式與GDPR有所扞格，有論者認為臺灣區分蒐集主體之二分立法方式，將造成對於「公務機關」之約束與限制較低，而對非公務機關之約束、限制較高。[121]然而，此種立法模式可能無助於清楚辨別控管者、受託運用者之主體身分與所應負擔義務。依GDPR規範架構，控管者須遵守負擔GDPR第5條之負擔與限制，包含「合法性、公平性、透明度」[122]、「資料最少蒐集原則」[123]、「正確性原則」[124]、以及「完整性與保密性原則」[125]及「課責性原則」[126]等。然而於我國個人資料保護法下，卻增加「公務機關」及「非公務機關」之二元區分，此種劃分方式可能不利於資料蒐集

[120] 李世德（2018），〈GDPR 與我國個人資料保護法之比較分析〉，《台灣經濟論衡》，第 16 卷第 3 期，頁 79。
[121] 楊智傑（2022），《個人資料保護法論》，初版，頁 40，臺北：元照。
[122] GDPR art 5.1(a): processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’).
[123] GDPR art 5.1(c): adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
[124] GDPR art 5.1(d): accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’).
[125] GDPR art 5.1(f): processed in a manner that ensures 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 (‘integrity and confidentiality’).
[126] GDPR art 5.2: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

主體之責任釐清。本文將於下段一併檢視我國個人資料保護法對於「受託運用者」之立法模式，並且同步分析之。

二、我國個人資料保護法未就「受託運用者」概念具體定義

我國個人資料保護法雖未定義「受託運用者」，然我國於「委託」蒐集、處理或利用個人資料者，具有「委託機關」之概念。如上所述，因受委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。[127]有論者認為此與GDPR下「受託運用者」概念相當。[128]又依據個人資料保護法施行細則第7條規定:「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之」;且依據個人資料保護法施行細則第8條第1項規定:「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。」然而，就形式而言，個人資料保護法施行細則並未明確要求委託機關應對受託者簽訂契約或其他法律文件之方式監督。僅於部分中央目的事業主管機關就所轄產業別發布之指定非公務機關個人資料檔案安全維護辦法中，可能進一步要求於委託契約或相關文件中，明確約定其內容。

就控管者與受託運用者之關係，依據個人資料保護法施行細則第8條第4項：「受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。」換言之，於我國個人資料保護法施行細則之規範下，亦明訂受託者蒐集、處理或利用個人資料不得逾越委託機關之指示。

針對外部責任之分配，法務部函釋認為，受委託機關僅為委託機關手足之延伸，受委託機關之行為應視同為委託機關之行為，倘受委託機關有違反個人資料保護法之情形，應由委託機關負賠償責

---

[127] 個人資料保護法第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

[128] 李世德，同前註 120，頁 79。

任。[129]

我國個人資料保護法既未於定義條款中明確區分「控管者」及「受託運用者」，僅透過法律條文內提出「受委託蒐集、處理或利用個人資料者」此一概念。自我國個人資料保護法第4條將委託蒐集、處理或利用個人資料者直接「視同委託機關」角度觀之，似將「控管者」與「受託運用者」間視為（內部）關係；反之，GDPR及控管者與受託運用者概念指引則認受託運用者係代表控管者運用個人資料之實體（GDPR及控管者與受託運用者概念指引明定受託運用者逾越控管者之指示時可能被視為控管者）。[130]

三、對受託者之監督形式要求

個人資料保護法施行細則第8條第1項要求委託機關應對受託者為適當之監督。[131]而於部分中央目的事業主管機關就所轄產業別發布之指定非公務機關個人資料檔案安全維護辦法中，可能有對於監督形式之進一步要求。例如金融監督管理委員會依據個人資料保護法第27條第3項規定[132]所發布之「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第8條第1項第6款提及：「非公務機關應就下列事項，訂定個人資料之管理程序：六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。」換言之，對受委託機關者監督之形式要求僅載於特定主管機關指定之非公務機關，而非一體適用於所有適用個人資料保護法之公務機關及非公務機關。

---

[129] 法務部 102 年 3 年 12 日法律字第 10100250980 號函、103 年 11 月 18 日法律字第 10303511950 號函及 104 年 10 月 23 日法律字第 10403513240 號函。

[130] EDPB, *supra* note 73, at 26.

[131] 個人資料保護法第 8 條第 1 項：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。」

[132] 個人資料保護法第 27 條：「（第一項）非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏；（第二項）中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法；（第三項）前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」

此外，個人資料保護法施行細則8條第2項明定委託機關對受委託機關應監督之內容，應包含下列事項：「一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間；二、受託者就第十二條第二項採取之措施；三、有複委託者，其約定之受託者；四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施；五、委託機關如對受託者有保留指示者，其保留指示之事項；六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」

其中，委託機關對受委託機關監督內容應包含個人資料保護法施行細則第12條第1項所指之「適當安全維護措施」、「安全維護事項」、或「適當安全措施」，亦即「指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。」。同條第2項更列舉得涵蓋之監督事項，包含：「一、配置管理之人員及相當資源；二、界定個人資料之範圍；三、個人資料之風險評估及管理機制；四、事故之預防、通報及應變機制；五、個人資料蒐集、處理及利用之內部管理程序；六、資料安全管理及人員管理；七、認知宣導及教育訓練；八、設備安全管理；九、資料安全稽核機制；十、使用紀錄、軌跡資料及證據保存；十一、個人資料安全維護之整體持續改善等。上述事項與所欲達成之個人資料保護目的間，並應具有適當比例為原則。」

就此觀之，GDPR及控管者與受託運用者概念指引對受託運用者與控管者之間之關係所提出之管理重點，控管者同樣應確保受託運用者將執行適當的技術上與組織上方法，以便其運用活動符合GDPR的規定。相較之下，我國個人資料保護法施行細則已提供充分具體之受託運用者與控管者監督事項。然而，目前我國法制仍欠缺以下兩者：即(1)對於監督方式之形式（應以書面為之，並具備法律上拘束力）要求並未普遍性適用於公務機關及各產業之非公務機關，而僅仰賴中央目的事業主管機關個別發布之子法；以及(2)要求

委託契約不應僅重述法規條文，而應該包含更明確和具體之內容。

四、對於共同委託機關之義務與責任分配方式無明確之要求

GDPR及控管者與受託運用者概念指引規定共同控管者應明確商定各自應負義務與責任、界定應由其中何者負責回應當事人請求，並將各自應負義務通知當事人。然而，我國個人資料保護法、個人資料保護法施行細則並未有明確具體規範。換言之，我國就「共同委託機關」之定義以及釐清義務之責任並未被法規明確要求，如「共同委託機關」間怠於商定內部與外部責任歸屬，縱使已約定內部義務與責任，當事人可能未受通知或無從得知。

換言之，我國現行實務對於「共同委託機關」概念之認定、其責任歸屬以及對於當事人之保障，相較指引文件有所不足。因而，將可能造成「共同委託機關」之間權責不清，且對於當事人之相關權利無法及時有效行使。

五、我國個人資料保護法施行細則中對「複委託」之權利義務並未具體明確

個人資料保護法施行細則第8條第2項明定對受託者監督之內容，應包含：「三、有複委託者，其約定之受託者。」因此，我國對於複委託關係，似乎限於「特定」之複委託。不若GDPR及控管者與受託運用者概念指引區分「概括授權」與「事前書面授權」之關係。

就監督關係而言，GDPR及控管者與受託運用者概念指引直接要求受託運用者與次受託人應簽訂契約，以課予次受託人對於第一個受託運用者所加諸之相同義務。[133]此外，無論「控管者所建議（對次受託人）之篩選標準為何，受託運用者應為次受託人義務的履行，對控管者負全部責任。」[134]然而，除要求明定複委託者外，我國個

[133] EDPB, *supra* note 73, at 43.
[134] EDPB, *supra* note 73, at 43.

人資料保護法並未明確規範受委託機關與複委託者之法律關係與監督形式要求，更未直接課與受委託機關相關法律義務。因之，我國個人資料保護法對於「複委託」或所謂「次受託人」並未有足夠具體之規範。

雖個人資料保護法對複委託關係之規範密度較低，民法對委任之規定或可做為參考。依據民法第537條規定「受任人應自己處理委任事務。但經委任人之同意或另有習慣或有不得已之事由者，得使第三人代為處理」；又民法第538條第1項規定「受任人違反前條之規定，使第三人代為處理委任事務者，就該第三人之行為，與就自己之行為，負同一責任。」同條第2項規定「受任人依前條之規定，使第三人代為處理委任事務者，僅就第三人之選任及其對於第三人所為之指示，負其責任。」因之，從民法之規定可推知，原則上受委託機關不得複委託他人處理個人資料，且除非委託機關同意複委託，否則受委託機關將與該第三人負同一責任。此外，於得同意複委託他人處理個人資料之情形，受委託機關則僅就其對第三人所為之指示負責。

依據既有複委託關係之法律原則，似乎無法推論出與控管者與受託運用者概念指引同等具體之義務。綜上，雖民法委任規定似有助於釐清個人資料保護法施行細則之複委託關係，然而，不若歐盟以個人資料保護法律明確規範責任，我國個人資料保護法施行細則僅要求明定「複委託者，其約定之受託者」對於後續的法律權利義務關係則未臻明確，且主管機關亦無法藉由民法規定對於相關主體進行監督。因而，我國個人資料保護法下之複委託關係，主要僅得透過內部監督或民事關係作為主要依據。為更明確化權利義務，主管機關或可考慮於個人資料保護法施行細則第8條第2項中將複委託法律關係與義務規範更為明確。

第四節 小結

針對以上議題，我國主管機關得考量整體規範情形與整體可行性，嘗

試進行下列法規調適：

一、針對「委託機關」與「受託者」予以具體定義

於我國個人資料保護法體系下，「委託機關」與「受委託機關」之定義並不明確，且兩者之間權責、監督義務之分配並未具體。針對兩者之定義，於不改變既有「公務機關」與「非公務機關」二分法之前提下，建議於個人資料保護法施行細則第7條[135]中，仿效GDPR及控管者與受託運用者概念指引之內容新增對於「委託機關」與「受委託機關」之主要區分判斷標準。並且得透過發布指引或函釋之模式，仿歐盟控管者與受託運用者概念指引中之案例方式說明，俾使業者得有更明確之參考指標。

二、於個人資料保護法施行細則第8條第1項新增對受託者監督形式要求

針對對受託者之監督形式要求，建議於個人資料保護法施行細則第8條第1項[136]新增：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督，並於委託契約或相關文件中，明確約定其內容。」俾將各別中央目的事業主管機關頒布之非公務機關個人資料檔案安全維護辦法內容擴大至各產業。

三、將共同委託機關義務與責任分配方式予以明文化

對於共同委託機關之義務與責任分配方式，建議於施行細則中增訂或透過發布函釋之方式，補充個人資料保護法第8條告知事項之細節。亦即個人資料保護法第8條「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：五、當事人依第三條規定得行使之權利及方式。」；其中「當事人依第三條規定得行使之權利及方式」應包含如有共同委

[135] 個人資料保護法施行細則第 7 條：「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」

[136] 個人資料保護法施行細則第 8 條第 1 項：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。」

託機關時，應明確告知當事人得行使之權利之對象。

四、於個人資料保護法施行細則第8條第2項第3款新增具體義務內容

針對個人資料保護法「複委託」之權利義務，建議於8條第2項第3款[137]增加以下文字：「三、有複委託者，其約定之受託者。並於複委託契約或相關文件中，明確約定複委託者應負與原受託者相同義務;原受託者應為複委託者義務之履行,對委託機關負全部責任。」

[137] 個人資料保護法施行細則第 8 條第 2 項：「前項監督至少應包含下列事項：
一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
二、受託者就第十二條第二項採取之措施。
三、有複委託者，其約定之受託者。
四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
五、委託機關如對受託者有保留指示者，其保留指示之事項。
六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」

第三章 GDPR被遺忘權於搜尋引擎案例適用標準之指引（Guidelines 5/2019）[138]

第一節 簡介

EDPB於徵詢公眾意見後於2020年7月通過「GDPR被遺忘權於搜尋引擎案例適用標準之指引」（下稱「**被遺忘權指引**」）。

刪除權並非GDPR所原創。歐盟層級中與當事人刪除權相關之法律規範，可見於歐盟資料保護指令第12(b)條[139]，該條責令成員國應賦予當事人於資料運用違反指令規定、資料不完整或不正確時，請求刪除之權利。此外，資料保護指令第14.1(a)條[140]亦責令成員國在特定情形下應賦予當事人針對資料運用之拒絕權，此拒絕權得作為成立被遺忘權之事由[141]。

從上述資料保護指令條文出發，歐盟法院於2014年5月3日作成Costeja判決[142]，特別肯認當事人對於搜尋引擎得主張被遺忘權，此乃被遺忘權一詞為世所知之濫觴。2016年4月歐盟制定之GDPR正式將「被遺忘權」一詞作為歐盟法條中之法律概念，並在資料保護指令及歐盟法院Costeja判決基礎上，更全面地規範當事人得主張被遺忘權之個別事由（GDPR第17.1條）及不適用該事由之例外（GDPR第17.3條）。惟GDPR第17.1條及17.3條中所使用之法律概念仍十分抽象，考量到當事人依GDPR第17.1條規定主張被遺忘權之情形，多涉及搜尋引擎提供之搜尋服

---

138 EDPB, '*GUIDELINES 5/2019 ON THE CRITERIA OF THE RIGHT TO BE FORGOTTEN IN THE SEARCH ENGINES CASES UNDER THE GDPR (PART 1)*', 7 July 2020 (Version 2.0).

139 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 (Directive 95/46/EC) art 12(b): Member States shall guarantee every data subject the right to obtain from the controller:…as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.

140 Directive 95/46/EC art 14.1(a): Member States shall grant the data subject the right:…at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data…

141 EDPB, *supra* note 138, at para 5.

142 The Court of Justice of the European Union (CJEU), Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014.

務，EDPB特作成此被遺忘權指引，就GDPR第17.1條及17.3條當事人得主張被遺忘權之事由及該事由之例外（即豁免事由），提供更明確具體之說明。

第二節 內容摘要

被遺忘權指引主要分為三部分，第一部分為導言，第二部分討論當事人得依據GDPR第17.1條行使去列表權之事由，第三部分討論依據GDPR第17.3條規定例外無須接受去列表權之事由。

一、導言

導言就些許概念進一步進行區辨與釐清，說明如下：

(一) 去列表權之權利內涵

被遺忘權指引所探討之主題，為在GDPR第17條下，應如何評估當事人依GDPR第17.1條向搜尋引擎所主張之去列表（delisting）權[143]。「去列表請求」意指當事人向搜尋引擎請求將以其姓名為搜尋條件之搜尋結果自搜尋列表中刪除。在概念上應區別者，對搜尋引擎行使去列表權，不代表能將當事人之資料完全自網路刪除。當事人之資料仍可能繼續存在於原始網路刊登者（如網路媒體）所經營之網站。此外，對搜尋引擎行使去列表權，並不使有關當事人之資料完全自搜尋列表中刪除。如以當事人姓名以外之關鍵字為搜尋條件，仍有可能搜尋至相關資料。

(二) 排除於被遺忘權指引討論範圍之事項

被遺忘權指引主要討論GDPR第17條適用於搜尋引擎作為資料運用者之情形。GDPR第17條對於其他控管者之適用，則不在被遺忘權指引探討範圍內。被遺忘權指引亦不處理GDPR第17.2規定所課予控管者通知義務之問題。惟於當事人向搜尋引擎請求將其個人

143 EDPB, *supra* note 138, at para 6.

資料去列表之情形，被遺忘權指引引用第29條工作小組（Article 29 Data Protection Working Party）意見認為，如搜尋引擎將當事人之資料自搜尋列表刪除，無須將刪除之事實告知儲存該資料之網站管理員。

二、GDPR第17.1條各款被遺忘權成立事由

(一) 資料已欠缺運用必要性（GDPR第17.1(a)條）

如當事人資料開放存取之時間超過搜尋引擎運用所需之時間時，當事人得基於隱私保護請求刪除與其個人相關之資料，另一方面，應同時考量網路使用者因搜尋引擎之搜尋服務而得更容易近用（access）資料之利益，並於兩者之間取得平衡，在此過程中，尤其應評估個人資料是否因時間經過而過時或未更新。

(二) 當事人撤回同意（GDPR第17.1(b)條）

此事由甚少適用當事人直接向搜尋引擎行使去列表權之情形。因當事人之同意必須特定，且與運用之行為明確相關，當事人發出同意之對象多為將資料刊登於網站之原始刊登者，而非將該資料編入搜尋索引、建立列表之搜尋引擎。惟如當事人向原始刊登資料於網路者撤回同意時，該網路刊登者有義務依GDPR第17.2條通知搜尋引擎，此時當事人仍得依GDPR第17.1(c)條請求搜尋引擎將其個人資料自搜尋列表中除去。

(三) 當事人拒絕資料之運用（GDPR第17.1(c)條）

依此條，如當事人依GDPR第21.1條反對特定運用資料之行為，當事人亦得同時向搜尋引擎行使去列表權。GDPR第21.1條之拒絕權，雖早先已見於資料保護指令第14.1(a)條，但GDPR第21.1條相較於資料保護指令第14條，減輕當事人於行使拒絕權時應負之舉證責任，當事人僅需要證明其行使拒絕權係源於與自身特定處境有關之事由，而控管者於拒絕刪除個人資料之情形，則應證明該拒絕行為

具有足以凌駕當事人權益之必要正當事由（compelling legitimate grounds）。

就此，被遺忘權指引肯認歐盟法院Costeja判決、歐洲人權法院在過往媒體事件中之判決、第29條工作小組關於歐盟法院Costeja判決所發展出之判準具有參考價值。被遺忘權指引也針對當事人得主張之與自身相關之「特定事由」提供些許例示。

(四) 資料遭違法運用（GDPR第17.1(d)條）

違反之法律除了GDPR本身之條文外，亦包括違反其他法規範，如個別國家法律或或搜尋結果遭法院命令禁止之情形。如搜尋引擎不能證明運用資料之法律依據，亦可能有本事由之適用。

(五) 因遵循法令而須刪除資料（GDPR第17.1(e)條）

遵循法令之情形包括法院禁制令、國家或歐盟法律明確規定之刪除義務、搜尋引擎違反保留期限等。

(六) 資料蒐集原因在於提供孩童資訊社會服務（GDPR第17.1(f)條）

本事由係為保護兒童而設之特別規定。被遺忘權指引表示，參照歐洲議會及理事會2000/31/CE指令序文，發生於網路上之經濟活動，即屬於資訊社會服務，其中亦包括提供線上搜尋、存取及檢索資料之服務。因此，搜尋引擎所提供之服務，很可能落入資訊社會服務之範圍。此外，被遺忘權指引認為，當事人依此條行使去列表權時，應肯認作為兒童乃GDPR第17.1(c)條連結至GDPR第21條之「與其自身特定處境相關之事由」。

三、GDPR第17.3條例外豁免事由

在搜尋引擎得援引GDPR第17.3條例外不刪除事由之情形，該事由得充作GDPR第17.1(c)條（即因行使拒絕權而得主張被遺忘權之情形）之必要正當事由。

(一) 處理資料為行使表意與資訊自由所必要（GDPR第17.3(a)條）

GDPR第17.1條賦予當事人之刪除權，並非絕對之權利，在衡量是否允許當事人刪除資料之申請時，除了利害關係人之權利外，也應考量包括存取資料自由在內之表意自由，並依比例原則，在不同之權利與自由間，取得平衡。特別是在以當事人姓名作為搜尋之方法時，對當事人隱私權及資料保護之侵害可能特別嚴重。

被遺忘權指引同意先前歐盟法院Costeja案判決之見解，認為當事人隱私權及個人資料之保護，原則上凌駕於網路使用者存取資料之利益。具體個案之評估上，可能因為諸如資料性質、資料敏感程度、利害關係人於公共生活中所扮演之角色在內之各種因素，而有所不同。此外，當事人請求之對象係針對以言論自由作為其活動核心之網路刊登者，抑或該請求是針對以建立個人資料為首要利益之搜尋引擎，於評價上也有所不同。搜尋引擎必須證明將特定內容列入搜尋結果乃絕對必要（strictly necessary）。

(二) 運用資料係控管者為遵守法律義務、執行基於公共利益之任務或行使公權力所必要（GDPR第17.3(b)條）

在大部分情形法律並不會強制搜尋引擎應刊載或散布某些資訊。法律通常係將此義務加諸於刊載特定內容之網頁，而搜尋引擎本身並不生產這些特定資訊。但如確實有成員國之法律課予搜尋引擎刊載或散布之義務，則搜尋引擎得援引此一豁免事由。考量搜尋引擎具有使網路使用者輕易存取網頁資料之功能，如特定資料依法須刊登於特定網頁，於評估當事人得否對搜尋引擎行使去列表權時，須考量該課予網頁刊登法律義務背後所代表之網路使用者存取資料利益。

(三) 公共衛生領域中之公共利益作為正當理由（GDPR第17.3(c)條）

GDPR第17.3(c)條中之「公共衛生」為第17.3(b)條「公共利益」之具體情形。搜尋引擎主張此豁免事由之合法性，必須先由歐盟法

律或成員國法律予以建立。被遺忘權指引認為，殊難想像保留包含特定當事人姓名之搜尋結果與搜尋引擎所主張公共衛生領域中之公共利益有任何關係。如果以其他搜尋條件得檢索至相關資訊，則保留以當事人姓名作為搜尋條件之搜尋結果並無必要。

(四) 為公共利益建檔之目的、科學或歷史研究之目的或統計之目的（GDPR第17.3(d)條）

搜尋引擎必須證明去列表將完全阻礙科學或歷史研究目的或統計目的之實現，且該科學或歷史研究目的必須客觀存在（非僅是搜尋引擎用戶主觀之研究或統計目的），且保留包含當事人姓名之搜尋結果與該目的之達成必須具有必要性，並應衡量當事人之權利與網路使用者透過搜尋引擎存取資料之利益。

(五) 為建立、行使或防禦法律上之請求（GDPR第17.3(e)條）

此規定不太可能作為搜尋引擎所得援引之豁免事由。

第三節 與我國個人資料保護法之重點比較

我國個人資料保護法已有當事人得向公務機關或非公務機關行使資料刪除權之規定。依照個人資料保護法第2條第8款[144]，非公務機關指公務機關以外之自然人、法人或其他團體。依此定義，搜尋引擎服務供應商為非公務機關。搜尋引擎雖非刊登資料內容於網路者，然其利用自動化爬蟲程式，將刊登於網路上之內容編入索引、儲存於伺服器，並於網路使用者使用搜尋引擎時，排序搜尋結果供網路使用者查閱等行為，已構成個人資料保護法第2條第3款、第4款[145]之蒐集、處理行為[146]而有個人資料保護法之適用。

---

144 個人資料保護法第 2 條第 8 款規定：「非公務機關：指前款以外之自然人、法人或其他團體。」

145 個人資料保護法第 2 條第 3 款、第 4 款規定：「三、蒐集：指以任何方式取得個人資料。四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。」

146 最高法院民事判決 109 年度台上字第 489 號判決理由。

依循被遺忘權指引之討論架構，以下說明現行個人資料保護法中當事人請求刪除之事由及豁免之事由。此外，個人資料保護法第11條第2項規定[147]之請求停止處理或利用權雖非刪除權，然使搜尋引擎停止將個人資料編入索引及呈現於搜尋列表，亦可達到將個人資料移除搜尋列表之結果[148]，因此，本文亦將併同討論個人資料保護法第11條第2項當事人之權利。

一、我國個人資料保護法中賦予當事人請求停止處理、利用、刪除之依據

個人資料保護法第11條第2項、第3項[149]、第4項[150]規定三種當事人得向公務機關或非公務機關請求停止處理或利用或刪除個人資料之情形：(1)個人資料正確性有爭議、(2)個人資料蒐集之特定目的消失或期限屆滿、及(3)個人資料之蒐集、處理、利用違反個人資料保護法之規定。個人資料保護法第19條第1項第7款[151]特別針對非公務機關規定，如非公務機關係自一般可得之來源取得個人資料，於當事人有更值得保護之重大利益時，當事人得禁止非公務機關處理或利用該個人資料，並依同條第2項[152]請求刪除，有學者認個人資料保護法第19條第1項第7款及同條第2項可適用於搜尋引擎利用自動搜尋程式自網路上蒐集各連結並予以列表之情形[153]，可謂是個人資料保

147 個人資料保護法第 11 條第 2 項規定：「個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。」

148 楊智傑（2015），〈個人資料保護法制上「被遺忘權利」與「個人反對權」：從 2014 年西班牙 Google v. AEPD 案判決出發〉，《國會月刊》，第 43 卷 7 期，頁 38。

149 個人資料保護法第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」

150 個人資料保護法第 11 條第 4 項規定：「違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。」

151 個人資料保護法第 19 條第 1 項第 7 款規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」

152 個人資料保護法第 19 條第 2 項規定：「蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。」

153 范姜真媺（2016），《網路時代個人資料保護之強化－被遺忘權利之主張》，興大法學，

護法中第4種刪除之事由。

個人資料保護法施行細則第20條[154]例示蒐集個人資料之特定目的消失之情形，在非公務機關之情形，除了因其歇業、解散或所營事業項目變更外，上開特定目的之消失，指(1)蒐集資料之特定目的已達成而無繼續處理或利用之必要，或(2)有其他事由足認該特定目的已無法達成或不存在者。

我國個人資料保護法及個人資料保護法施行細則規定之請求停止處理、利用、刪除事由及法律依據整理如下表：

刪除事由	法律依據
個人資料正確性有爭議。	個人資料保護法第 11 條第 2 項
個人資料蒐集之特定目的消失或期限屆滿，蒐集之特定目的消失包括： ➢ 公務機關經裁撤或改組而無承受業務機關。 ➢ 非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。 ➢ 特定目的已達成而無繼續處理或利用之必要。 ➢ 其他事由足認該特定目的已無法達成或不存在。	個人資料保護法第 11 條第 3 項、個人資料保護法施行細則第 20 條
個人資料之蒐集、處理、利用違反個人資料保護法規定。	個人資料保護法第 11 條第 4 項

第 19 期，頁 92。

[154] 個人資料保護法施行細則第 20 條規定：「本法第十一條第三項所稱特定目的消失，指下列各款情形之一：一、公務機關經裁撤或改組而無承受業務機關。二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。三、特定目的已達成而無繼續處理或利用之必要。四、其他事由足認該特定目的已無法達成或不存在。」

個人資料取自於一般可得之來源，且當事人具有更值得保護之重大利益。	個人資料保護法第 19 條第 1 項第 7 款及同條第 2 項

二、我國個人資料保護法所規定例外無須刪除之豁免事由

個人資料保護法第11條第2項請求停止處理及利用權、第3項刪除權分別設有如下豁免事由：在個人資料保護法第11條第2項資料之正確性有爭議之情形，如(1)處理或利用係因執行職務或業務所必須，或(2)處理或利用經當事人書面同意，並經註明其爭議者，控管者無須停止處理或利用（個人資料保護法第11條第2項但書）。在個人資料保護法第11條第3項個人資料蒐集之特定目的消失或期限屆滿之情形，如(1)係因執行職務或業務所必須，或(2)經當事人書面同意者，控管者無須刪除、停止處理或利用資料（個人資料保護法第11條第3項但書）。

個人資料保護法施行細則第21條[155]針對個人資料保護法第11條第3項但書中之「因執行職務或業務所必須」之例外事由解釋為：(1)有法令規定或契約約定之保存期限、(2)有理由足認刪除將侵害當事人值得保護之利益、(3)其他不能刪除之正當事由。

我國個人資料保護法及個人資料保護法施行細則規定之豁免事由整理如下表：

豁免事由	法律依據
處理或利用係因執行職務或業務所必須。個人資料保護法施行細則針對「因執行職務或業務所必須」之解釋為： • 有法令規定或契約約定之保存期限。	個人資料保護法第 11 條第 2 項、第 3 項但書、個人資料保護法施行細則第 21 條

[155] 個人資料保護法施行細則第 21 條規定：「有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。」

豁免事由	法律依據
• 有理由足認刪除將侵害當事人值得保護之利益[156]。 • 其他不能刪除之正當事由。	
經當事人書面同意。	個人資料保護法第 11 條第 2 項、第 3 項但書

三、我國個人資料保護法規定與GDPR規定之比較

(一) 刪除、停止處理、利用事由部分

與GDPR第17.1條規定之刪除事由相比，在法律層次上，我國個人資料保護法第11條第2項至第4項規定缺少了如下事由：

- 當事人撤回對資料蒐集、處理、利用之同意（GDPR 第 17.1(b)條）；
- 當事人因其自身特定處境行使拒絕權（GDPR 第 17.1(c)條）；
- 資料控管人因遵守法律負有刪除義務（GDPR 第 17.1(e)條）[157]；
- 兒童使用資訊社會服務之特別刪除權作為刪除事由（GDPR 第 17.1(f)條）。

於個人資料遭違法運用之情形，我國個人資料保護法第11條第4項僅以「違反本法」作為請求刪除、停止處理或利用之要件，而非如GDPR第17.1(d)條規定及被遺忘權指引對於「違法」採取廣義解釋，包括GDPR以外之各種法律規定，似保障不周。就此，目前似僅能藉由對個人資料保護法第5條如「應尊重當事人權益」、「誠實及

[156] 此款豁免事由似僅在公務及非公務機關主動刪除個人資料或停止處理或利用資料之情形始有意義，故 不在本文討論範圍。

[157] 個人資料保護法第 11 條第 3 項中以「蒐集資料期限屆滿」作為當事人得請求刪除之事由，僅為被遺忘權指引第 38 段針對 GDPR 第 17.1(e)條「因遵守法律義務而刪除」之一種情形。

信用方法」等基本原則著手，擴大解釋「違反個人資料保護法」之範圍[158]。

就上述規範空白之處，儘管個人資料保護法施行細則第20條第4款對於第11條第3項之特定目的消失之要件設有「其他事由足認該特定目的已無法達成或不存在」之概括條款，如所涉及之案件基礎事實與「特定目的無法達成或不存在」無關，則當事人似難援引個人資料保護法施行細則第20條第4款行使刪除權之概括事由。

1. 在我國個人資料保護法下以撤回同意作為行使去列表權事由

GDPR第17.1(b)條撤回同意之情形雖未規定於個人資料保護法第11條第2項至第4項，然個人資料保護法第15條第2款[159]、第16條第7款[160]、第19條第1項第5款[161]、第20條第1項第6款[162]皆有以當事人同意作為公務機關及非公務機關蒐集、處理、利用資料正當事由之規定。當事人撤回上述條文之同意後，如蒐集個人資料之特定目的或要件已不存在，當事人得依個人資料保護法第11條第3項向資料管控者請求停止蒐集、處理或利用該個人資料[163]。不過與被遺忘權指引所述者類似，在大部分當事人向搜尋引擎行使去列表權之情形，當事人最初同意之對象為原始資料刊登者，而非搜尋引擎，因此當事人也無從對搜尋引擎撤回同意。

---

158 范姜真媺，同前註 153，頁 94。

159 個人資料保護法第 15 條第 2 款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：二、經當事人同意。」

160 個人資料保護法第 16 條第 7 款規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：七、經當事人同意。」

161 個人資料保護法第 19 條第 1 項第 5 款規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：五、經當事人同意。」

162 個人資料保護法第 20 條第 1 項第 6 款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：六、經當事人同意。」

163 法務部 106 年 11 月 10 日法律字第 10603512680 號函。

2. 在我國個人資料保護法下當事人因自身特定處境行使拒絕權及刪除權

個人資料保護法第11條第2項至第4項並未規定如GDPR第17.1(c)條賦予當事人於因其自身處境行使拒絕權時亦得請求刪除之權利。惟在當事人對搜尋引擎行使去列表權之情形，如搜尋引擎蒐集、處理個人資料之事由係源於個人資料保護法第19條第1項第7款規定，該規定特別容許當事人於有更值得保護之重大利益時，得禁止處理或利用該資料，並依同條第2項向蒐集及處理者請求刪除、停止處理或利用。此規定頗有資料保護指令第14.1(a)條之影子，亦即當事人於行使去列表權時，必須先證明有比資料之處理與利用更值得保護之重大利益。但如前所述，在GDPR第17.1(c)條及GDPR第21.1條規定下，當事人僅需舉證係因自身特定處境反對資料之運用即可，如搜尋引擎欲繼續運用該資料，則須證明該運用具有「必要正當事由」，由此觀之，舉證責任有所不同。

3. 在我國個人資料保護法下當事人主張搜尋引擎因遵守法律義務或資料運用違法而需刪除資料之去列表權

如前所述，我國個人資料保護法第11條第4項係以「違反個人資料保護法」作為當事人得請求刪除個人資料之事由，而非「違反法律」。範圍稍嫌狹隘。雖個人資料保護法第11條第3項規定之「期限屆滿」亦得適用於蒐集、處理、利用資料法定期限屆滿之情形，然無法包含所有須遵守法律義務之情形。

4. 當事人以個人資料保護法第11條第3項「特定目的無法達成或不存在」作為向搜尋引擎行使去列表權事由之問題

在當事人依個人資料保護法第11條第3項規定向搜尋引擎行使去列表權之情形，有文獻提及因搜尋引擎蒐集網路上資訊，編入索引、存入伺服器等行為，目的在使網路使用者更便利地蒐

用資料，此目的並不會隨著時間經過而消失，是將個人資料保護法第11條第3項規定「特定目的無法達成或不存在」之要件適用於對搜尋引擎行使去列表權之情形，會有一定之困難[164]。就此，被遺忘權指引於解釋GDPR第17.1(a)條時表示，此時重點應在保護隱私及網路使用者近用資訊之利益間取得平衡，尤其必須評估隨著時間過去，資料是否已經過時或未更新[165]，而非專以搜尋引擎蒐集資料之目的為主。此意見可供我國法解釋參考。

5. 個人資料保護法欠缺以保護兒童資料為目的之行使去列表權事由

GDPR第17.1(f)條賦予兒童特別之保護，被遺忘權指引另明確指出，兒童亦得循GDPR第17.1(c)條規定向搜尋引擎行使去列表權。此為保護兒童而設之事由為我國所欠缺。

(二) 豁免事由部分

1. 法定豁免事由

與GDPR第17.3條豁免事由相比，我國個人資料保護法規定於法律層次之豁免事由較為限縮，僅「因執行職務或業務所必須」及「經當事人書面同意」。

GDPR並未以「經當事人書面同意」作為豁免刪除權之事由。我國個人資料保護法以「經當事人書面同意」為豁免事由，似乎亦無必要。如條文係指該當事人之書面同意發生於當事人於行使第11條第2項及第3項權利之後，因當事人依個人資料保護法第11條第2項或第3項行使刪除權或請求停止蒐集或處理，已隱含當事人不同意資料管控者繼續對其個人資料之蒐集、處理、或利用之行為，殊難想像當事人事後又推翻自己主張。縱使當事人

[164] 張陳弘、莊植寧（2022），《新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明》，頁 229，臺北：新學林。
[165] EDPB, *supra* note 138, at para 19.

再次書面同意資料之蒐集、處理及利用，則公務機關或非公務機關本得再依個人資料保護法中相關規定再次蒐集、處理及利用，似無須將「經當事人書面同意」另行納入豁免事由。如條文係指當事人之書面同意發生於當事人於行使第11條第2項及第3項權利之前，是否意味著只要當事人曾書面同意資料之蒐集、處理或利用，當事人事後如行使刪除權、停止處理或利用之權，控管者即得一律主張豁免？由此觀之，以「經當事人書面同意」作為豁免事由並無必要，甚至反而不利於當事人行使權利。惟如前所述，當事人同意搜尋引擎蒐集當事人資料編入索引之情形，在對搜尋引擎行使去列表權之情形並不常見。

「因執行職務或業務所必須」相較於GDPR第17.3條各項豁免事由略顯空泛。在GDPR第17.3條諸多豁免事由中，多見「法定義務」、「為公共利益」等用語，被遺忘權指引亦強調如搜尋引擎主張係為公共利益、科學或歷史研究目的之建檔而不接受去列表權之行使，該目的之追求必須具有客觀性，非僅以搜尋引擎用戶主觀所追求之目的為主[166]。我國個人資料保護法第11條第2項、第3項但書規定之「因執行職務或業務」在文義上似乎更偏向公務機關及非公務機關自己判斷之「蒐集之特定目的」及該目的與資料之關聯性[167]。

被遺忘權指引亦強調衡量當事人隱私與個人資料之保護及公眾近用網路之利益時，須探究是否無須將當事人之姓名作為搜尋條件亦可達成相同目的，此必要性之審查似得作為依我國個人資料保護法第11條第2項、第3項中因執行職務或業務所「必須」要件之解釋。

2. 非法定之豁免事由

除了個人資料保護法第11條第2項、第3項及個人資料保護

[166] EDPB, *supra* note 138, at para 80.
[167] 范姜真媺，同前註 153，頁 94。

法施行細則規定之豁免事由。最高法院見解[168]認為：「是個人資料之蒐集、處理或利用，應合法、有特定目的，且不得逾越必要範圍。資訊主體對於曾經合法公開之個人資料，因時間經過，其被蒐集、處理或利用之特定目的已不存在，或已逾越該目的之必要範圍，自得請求該資料之蒐集或處理者予以刪除。關於必要性存否之認定，應就資訊主體之資訊隱私權與公眾知的權利之公共利益，為法益之衡量。」。是在法定事由之外，最高法院肯認「公眾知的權利」作為衡量當事人得否行使刪除權之事由。個人資料為他人刊登於網路上之內容時，行使刪除權亦將涉及我國憲法所保障之言論自由[169]，此二者可對應GDPR第17.3(a)條規定，可謂我國個人資料保護法未明文之非法定豁免事由。

3. 我國個人資料保護法豁免事由之缺漏

承上所述，我國個人資料保護法法律層次規範之豁免事由僅有「因執行職務或業務所必須」及「經當事人同意」，相較於GDPR第17.3條各款事由尚有不足，雖上述問題或可藉由解釋個人資料保護法施行細則第21條第1款之「有法令規定或契約約定之保存期限」或第3款中之「其他不能刪除之正當事由」予以彌補，惟仍可能產生法律明確性及法律保留原則之問題[170]。

GDPR第17.3條各款豁免事由得適用至所有當事人行使刪除權之情形。我國個人資料保護法之規範模式係針對個別刪除、停止處理、利用事由規定豁免事由，如此不僅導致重複規範（如「因執行職務或業務所必須」及「經當事人書面同意」於個人資料保護法第11條第2項、第3項重複規範兩次），亦將產生不同刪除事由之豁免事由間是否能夠流用之問題。例如，在個人資料保護法第11條第2項「個人資料正確性有爭議」之情形，如雇主遭

168 同前註 146。
169 王龍寬（2022），《淺論被遺忘權之基本權衝突》，萬國法律，第 243 號，頁 24。
170 張陳弘、莊植寧，同前註 164，頁 228。

勞動部依勞動基準法第80條之1規定[171]公告於違反勞動法令事業單位，該違反勞動法令事項尚在爭訟階段，而該雇主依個人資料保護法第11條第2項主張其遭公告之個人資料正確性有疑義，勞動部應停止處理、利用該個人資料。勞動部應可主張其對個人資料之處理及利用係「因執行職務或業務所必須」，具有不停止處理、利用之正當事由。惟個人資料保護法施行細則並未針對個人資料保護法第11條第2項之「因執行職務或業務所必須」作更進一步的解釋，個人資料保護法施行細則第21條針對個人資料保護法第11條第3項「因執行職務或業務所必須」的解釋，是否亦可適用於個人資料保護法第11條第2項即有疑義。

[171] 勞動基準法第 80 條之 1 第 1 項規定：「違反本法經主管機關處以罰鍰者，主管機關應公布其事業單位或事業主之名稱、負責人姓名、處分期日、違反條文及罰鍰金額，並限期令其改善；屆期未改善者，應按次處罰。」

第四節 小結

以下將上述分析提及我國個人資料保護法相較於GDPR不足或有疑義之處整理如下表，並提出相關之可能解決方法：

	GDPR 規範	我國個人資料保護法不足或有疑義之處	可能之解決方法
規範方式	全部豁免事由皆列於 GDPR 本文。	明示於我國個人資料保護法之豁免事由僅「因執行職務或業務所必須」或「經當事人書面同意」，概括事由列於個人資料保護法施行細則，產生法律明確性及法律保留原則之問題。	修正個人資料保護法。
	豁免事由可流用於全部行使刪除權事由。	豁免事由不能流用於不同行使刪除權事由。	修正個人資料保護法。
	未將「經當事人書面同意」作為豁免事由。	將「經當事人書面同意」作為豁免事由似無必要。	刪除「經當事人書面同意」豁免事由。
行使刪除	個人資料就蒐集或以其他方式運用之目的而言已無必要（GDPR 第 17.1(a)條）。	得適用我國個人資料保護法第 11 條第 3 項規定。惟搜尋引擎「蒐集	➢ 適當地解釋個人資料保護法第 11 條第 3 項規定。

	GDPR 規範	我國個人資料保護法不足或有疑義之處	可能之解決方法
		資料之商業目的」並不會因時間而消失。	➢ 參考遺忘權指引對 GDPR 第 17.1(a)條之解釋，重點應在保護隱私及網路使用者近用資訊之利益間取得平衡，非專以搜尋引擎蒐集資料之目的為主。
	當事人撤回對資料蒐集、處理、利用之同意（GDPR 第 17.1(b)條）。	我國個人資料保護法無明文規定。	如當事人撤回同意，且蒐集個人資料之特定目的或要件已不存在，當事人得依據個人資料保護法第 11 條第 3 項請求刪除。
	當事人因其自身特定處境行使拒絕權（GDPR 第 17.1(c)條）。	在個人資料係源於一般可得之來源時，得適用我國個人資料保護法第 19 條第 1 項第 7 款、第 2 項規定之拒絕權、刪除權、及停止處理或利用權。惟現行規定要求當事人舉證有更值得保護之重大利益。	如欲改變當事人與搜尋引擎間之舉證責任，須修正個人資料保護法。
	當事人個人資料遭違法運用（GDPR 第 17.1(d)條）。	我國個人資料保護法第 11 條第 4 項僅以「違反本法」作為請求刪除、停止處理或利用之要件。	➢ 修正個人資料保護法。 ➢ 於修正個人資料保護法前，擴大個人資料保護法第 5 條之適用，

	GDPR 規範	我國個人資料保護法不足或有疑義之處	可能之解決方法
			如不符個人資料保護法第 5 條之蒐集、處理或利用，即構成個人資料保護法第 11 條第 4 項之「違反本法」。
	控管者負有法定刪除義務（GDPR 第 17.1(e)條）。	我國個人資料保護法第 11 第 3 項、第 4 項規定不能涵蓋所有控管者負有法定刪除義務之情形。	➢ 修正個人資料保護法。 ➢ 於修正個人資料保護法前，擴大個人資料保護法第 5 條之適用，如不符個人資料保護法第 5 條之蒐集、處理或利用，即構成個人資料保護法第 11 條第 4 項之「違反本法」。
	兒童使用資訊社會服務之特別刪除權（GDPR 第 17.1(f)條）。	我國個人資料保護法無針對兒童之特別規定。	修正個人資料保護法。
豁免事由	為行使表意及資訊自由之權利（GDPR 第 17.3(a)條）。	我國個人資料保護法無明文規定。	透過憲法對基本權利之保障予以補充。
	遵守法定義務、為公共利益執行職務、為行使公權力（GDPR 第 17.3(b)	我國個人資料保護法第 11 條第 2 項、第 3 項規定之「因執行職務或	主管機關得參考被遺忘權指引，強調該目的之追求必須具有客觀性，

	GDPR 規範	我國個人資料保護法不足或有疑義之處	可能之解決方法
	條)、為公共衛生領域之公共利益（GDPR 第 17.3(c)條）、為公共利益建檔之目的、科學或歷史研究之目的或統計之目的（GDPR 第 17.3(d)條）。	業務所必須」文義上過度偏重由公務機關或非公務機關自身追求之職務或業務目的。	且須探究是否無須將當事人之姓名作為搜尋條件即可達成相同目的。

第四章 當事人權利（近用權）指引（Guidelines 01/2022）[172]

第一節 簡介

EDPB於2022年1月18日通過「當事人權利（近用權）指引」（下稱近用權指引），近用權指引旨在釐清GDPR第15條當事人近用權（Right of access）之內涵，並針對GDPR第15條文意進一步解釋。所謂「當事人近用權」，係指當事人有權向控管者確認其個人資料是否正被運用；若有，則當事人有權接近使用其個人資料及相關資訊，包括運用之目的、個人資料所涉及之類型等[173]。

我國對於當事人之近用權相關保障，主要規定於個人資料保護法第3條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」及個人資料保護法第10條：「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」

無論是歐盟或我國，普遍接受當事人對控管者運用（蒐集、處理及利用）之資料具有近用權，惟對於近用權之內涵以及範圍不盡相同，是以，本文首先將介紹歐盟透過近用權指引對GDPR第15條所揭示之當事人近用權的內涵及具體實施細節；其次，將GDPR及近用權指引之內容與我國個人資料保護法運作進行比較。

---

[172] EDPB, '*GUIDELINES 01/2021 ON DATA SUBJECT RIGHTS—RIGHT OF ACCESS*', 18 January 2022 (Version 1.0).

[173] GDPR art 15.1: The data subject shall have the 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 and the following information: (a) the purposes of the processing, (b) the categories of personal data concerned…

第二節 內容摘要

依據近用權指引前言之介紹，近用權應與具有其他目標的類似權利有所區隔。當事人行使近用權時，毋須提出事由即可進行請求；控管者亦毋須分析該請求是否確實會協助當事人查驗相關運用之合法性或行使其他權利。近用權之行使屬個人權利，不以行使其他權利為先決條件，其他權利之行使亦不取決於是否行使近用權[174]。近用權包含三個不同面向：第一，確認個人資料是否已被運用；第二，近用該等個人資料；及第三，近用關於運用之資訊，如目的、資料類別及資料接收方、運用期間、當事人權利及關於移轉至第三國之適當保護措施等[175]。

近用權指引的架構分為五個部分，分別為「近用權之目的（GDPR第15條之架構）」、「關於近用請求評估之一般考量」、「近用權之範圍及其涉及之個人資料及資訊」、「控管者如何提供近用」，以及「近用權之限縮及限制」。以下將分述這五個部分之重點：

一、近用權之目的

近用權之目的係為使當事人能夠瞭解其個人資料之運用方式及運用之後果，並確認被運用資料之正確性。當事人透過行使近用權，將獲得充分、透明且易近用之資料運用（無論所採用技術為何）資訊，並使當事人能夠確認其資料之運用的合法性及正確性[176]。此外，近用權之行使屬個人權利，不以行使其他權利為先決條件，其他權利之行使亦不取決於是否行使近用權。控管者不應針對當事人「為何」行使近用權進行評估，而僅應評估當事人有「哪些」請求及其是否持有與該當事人相關之個人資料[177]。

歐盟當事人之近用權主要規範於GDPR第15條，第15條第1項及第15條第2項定義近用權內容，第15條第3項就近用之方式有所規範，第15條

[174] EDPB, *supra* note 172, at 9.
[175] EDPB, *supra* note 172, at 9.
[176] EDPB, *supra* note 172, at 9.
[177] EDPB, *supra* note 172, at 9.

第4項補充第12條第5項所定對所有當事人權利之限縮及限制，特別強調行使近用權時所涉他人權利及自由[178]。以下就針對GDPR第15條之架構進行分析：

條號	條文內容
第 15 條第 1 項前段	確認控管者是否正在運用請求人之個人資料[179]。
第 15 條第 1 項中段	近用與請求人相關之個人資料[180]。
第 15 條第 1 項後段	近用以下之運用相關資訊： (a) 運用之目的； (b) 個人資料類別； (c) 接收方或接收方之類型； (d) 設想之運用期限或判斷該期限之標準； (e) 更正權、刪除權、限制運用權及拒絕運用權之存在； (f) 向監管機關提出申訴之權利； (g) 於非直接向當事人蒐集資料的情況下，任何關於資料來源之可用資訊； (h) 自動化決策（包括剖析）之存在及其他相關資訊[181]。
第 15 條第 2 項	當個人資料被移轉至第三國或國際組織時，依據第 46 條實施保護措施之資訊。
第 15 條第 3 項前段	控管者提供其所運用個人資料之複製本的義務。

[178] EDPB, *supra* note 172, at 11.

[179] 亦可參 EDPB, *supra* note 172, at 11：「當事人於提出近用個人資料之要求時，首先必須確認控管者是否有運用其相關資料。……若控管者並未運用與請求近用之當事人相關的個人資料，所提供資訊將僅限於確認其並未運用與當事人相關之個人資料。若控管者確實有運用與當事人相關之資料，控管者必須向當事人確認此事實。此等確認得單獨傳達，亦得將其納入關於其運用個人資料之資訊中。」

[180] 亦可參 EDPB, *supra* note 172, at 11：「近用個人資料……與 GDPR 第 4 條第 1 項所定義之個人資料概念相關。除姓名及地址等個人基本資料外，只要屬於 GDPR 之實質範圍，特別是在運用方式上，各類資料均可能屬此定義範圍……近用個人資料於此係指實際近用個人資料本身，而非僅係個人資料之一般敘述，亦非僅係控管者所運用個人資料之類別。……提供近用資料之義務並非依據該等資料之類型或來源所影響。即使該等資料係由請求人直接向控管者提供，亦完全適用，因為其目的係為讓當事人知悉控管者對該等資料之實際運用情況。」

[181] 亦可參 EDPB, *supra* note 172, at 12：「提供關於運用及當事人權利之資訊，得擷取自例如控管者隱私權通知之文字，或自控管者之運用作業紀錄中摘取，惟可能必須進行更新並針對提出請求之當事人進行調整。」

第 15 條第 3 項中段	控管者依據其行政成本就當事人請求提供額外複製本收取合理費用。
第 15 條第 3 項後段	以電子形式提供資訊[182]。
第 15 條第 4 項	考量他人權利及自由。

二、關於近用權請求評估之一般考量

控管者應主動針對個人資料之近用請求（request）進行備置，亦即控管者應該準備受理請求，對其進行適當評估，並向請求人提供適當回覆，不得無故遲延。依據GDPR第24條，控管者應就近用請求進行充分且符合比例的準備，並將運用之性質、範圍、背景及目的，與對自然人權利及自由之風險納入考量[183]。

(一) 請求的範圍及認定

近用權指引說明，為辨認請求，控管者首先應該考慮以下五個問題：

問題[184]		近用權指引說明
1	請求是否涉及個人資料？	關於其他議題之資訊請求，包括關於控管者、其商業模式或其運用作業等與個人資料無關之一般資訊，均不能被視為依據 GDPR 第 15 條提出之請求。此外，關於匿名化資料或無涉請求人或提出請求之授權代理人所代表之人資料的資訊請求，均不屬近用權之範圍。而可與當事人連結之假名化資料亦應被視為屬於請求之範圍[185]。

[182] 亦可參 EDPB, *supra* note 172, at 13-14：「提供複製本之要求係指，應將提出請求人個人資料之相關資訊，以允許當事人保留所有資訊並重複閱覽的方式提供予當事人。……控管者不應將間接成本或其他一般費用轉嫁予當事人，而應將重點放在提供額外複製本所產生的具體費用上。於規畫此流程時，控管者應有效部署其人力及物力資源，以降低製作複製本之成本。」

[183] EDPB, *supra* note 172, at 18-19.

[184] EDPB, *supra* note 172, at 19-21.

[185] EDPB, *supra* note 172, at 19.

問題[184]		近用權指引說明
2	請求是否與請求人（或提出請求之授權代理人所代表之人）相關？	一般而言，一項請求僅能涉及提出請求人之資料。近用他人資料之請求僅得於已取得適當授權的情況下提出[186]。
3	除 GDPR 外，是否也適用其他規範特定類型資料近用之法規？	若控管者對當事人擬行使之權利有疑問，建議要求提出請求之當事人說明請求事項。與當事人進行此等溝通時，控管者仍有義務迅即採取行動，不得無故遲延。於有疑問的情況下，若控管者要求當事人進一步說明但卻未得到回應，控管者應以第一次請求中所提供之資訊為基礎進行解釋及採取行動，惟仍應謹記其有義務促使當事人行使近用權[187]。
4	請求是否屬第 15 條範圍？	若欲提出近用權請求，請求人僅需說明其欲知悉控管者運用哪些與其相關之個人資料。控管者不能以請求人並未說明其請求之法律依據而拒絕提供資料[188]。
5	當事人是否想近用其被運用資料之全部或一部？	若欲將當事人請求範圍限縮於 GDPR 第 15 條之特定條款，必須有明確的依據。例如，若當事人明確要求提供「其被運用資料之相關資訊」，控管者應假設當事人擬行使其於 GDPR 第 15 條第 1 項及第 2 項之全部權利[189]。

就請求之形式而言，GDPR本身並沒有規定，但依據第12條第3項，控管者收到請求的日期，原則上成為控管者需於一個月內提供其就該請求採取行動之相關資訊的起始日。EDPB認為良好的做法為，控管者應以書面形式確認收到請求，例如透過發送電子郵件（或透過

[186] EDPB, *supra* note 172, at 19.
[187] EDPB, *supra* note 172 at 20.
[188] EDPB, *supra* note 172, at 20-21.
[189] EDPB, *supra* note 172, at 19-21.

實體郵寄，如可行）予請求人，確認已收到其請求，及一個月期間起始日[190]。

雖GDPR亦未對識別當事人身分的方法提出任何規範，惟GDPR第11條及第12條規定行使所有當事人權利的條件[191]。控管者應依據當事人行使其個人權利之請求採取行動，除非其能提出符合課責性原則（the principle of accountability）之理由證明其無法識別當事人。控管者無義務僅為回覆請求而取得額外資訊來識別當事人。然而，控管者不應拒絕取得此等額外資訊[192]。

(二) 關於識別請求人之比例性評估

於控管者有合理事由懷疑請求人的身分時，控管者得要求提供額外資訊以確認當事人身分。由於控管者須確保其所蒐集的個人資料不會超出識別請求人身分所必須之範圍，故控管者應進行比例性評估，考量正在運用之個人資料類型、請求之性質、提出請求之背景，及任何可能因不當揭露而造成之損害。於評估比例性時，應確保避免過度蒐集資料[193]。於處理近用權請求之整個過程中，控管者應確保運用之安全性，包括例如為當事人備置提供額外資訊的安全管道。認證方式應具相關性、適當性、符合比例原則及資料最小化原則[194]。

考量到許多組織（如酒店、銀行、租車公司）會要求客戶提供身分證明文件複製本，一般而言，以上並非適當的認證方式。控管者得實施快速、有效的安全措施來識別其先前已完成認證的當事人，例如透過包含確認連結、安全問題或確認碼的電子郵件或簡訊[195]。若要求提供身分證明文件，控管者必須實施保護措施，防止非法運用身分證明文件。EDPB建議，良好的做法為，控管者應於確認身分證明文件後進行相關註記，例如「已查驗身分證明文件」，以避免不必要地複

190 EDPB, *supra* note 172, at 21-22.
191 EDPB, *supra* note 172, at 23.
192 EDPB, *supra* note 172, at 23.
193 EDPB, *supra* note 172, at 25.
194 EDPB, *supra* note 172, at 25.
195 EDPB, *supra* note 172, at 26.

製或儲存身分證明文件之複製本[196]。

(三) 透過第三人/代理人提出之請求

1. 代未成年人提出請求

近用權得由代理人或法定監護人代未成年人提出請求，於特定情況下，被授權行使近用權之人的身分及代表當事人行事之授權可能需要進行查驗[197]。兒童就其本身權利而言亦屬當事人，兒童近用權之行使，依個別兒童的成熟度及能力，決定是否由親權人代兒童提出[198]。因GDPR中對兒童個人資料之特別保護，控管者應採取適當措施，避免向未經授權之人揭露未成年人之個人資料[199]。親權人代表兒童行使之權利不應與資料保護法律以外之情況混為一談，於該等情況下，國家法規可能允許親權人詢問及取得關於兒童之資訊（例如，兒童在校表現）[200]。

2. 透過第三人提供之入口網站/管道行使近用權

有些公司提供可使當事人透過入口網站提出近用權請求之服務。當事人登入並連接至入口網站後，可透過該網頁提交如近用權、更正或刪除自不同控管者的資料等請求。於使用由第三人提供的入口網站時，會出現不同的問題。控管者需確保第三人係合法代表當事人行事，因其有必要確保不將資料揭露予未經授權之人[201]。

三、近用權之範圍及其涉及之個人資料及資訊

(一) 個人資料的定義

GDPR第15條第1項及第3項分別提及「個人資料」及「正在被運用之個人資料」。依據GDPR第4條第1項定義，所謂「個人資料」為

196 EDPB, *supra* note 172, at 27.
197 EDPB, *supra* note 172, at 27.
198 EDPB, *supra* note 172, at 28.
199 EDPB, *supra* note 172, at 28.
200 EDPB, *supra* note 172, at 28.
201 EDPB, *supra* note 172, at 28-29.

已識別或可識別身分之自然人之任何資訊，而所謂「可得識別自然人」人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具[202]。另應注意者為，有些資訊非屬GDPR之範圍，如匿名化資料，因其為不直接或間接與可識別身分之人相關的資料。例如，運用當事人個人資料之伺服器位置即非屬個人資料[203]。

在Nowak一案中，歐盟法院認定考生於專業考試中提交的書面答案及考官對該等答案之任何評論均構成該考生之個人資料。若該等資料其與當事人相關，則該等主觀資訊屬「意見及評價形式」之個人資料。因此，情境評估應檢視資訊對個人可能產生的影響或後果，從而判斷近用權的範圍[204]。

(二) 近用權之個人資料範圍

1. 關於他/她的個人資料

EDPB認為，如同第29條工作小組曾就資料可攜權所述，控管者不應以「過度限縮」的方式解釋「關於他/她的個人資料」。若當事人使用其中包括對話者個人資料之錄音作為其他目的（例如，發布該錄音），就運用錄音中通話對象之個人資料而言，當事人將成為控管者。雖然這不會免除控管者於適當分析是否得提供完整錄音之近用時之資料保護義務，但控管者應告知當事人，其於此情況下可能成為控管者[205]。

依據GDPR第29條，控管者應確保，依其授權行事且有權近用個人資料之人，除非係依據控管者之指示，不會運用個人資料。若該人為履行控管者指示以外之其他目的運用個人資料，則其可能成為該

202 EDPB, *supra* note 172, at 29-30.
203 EDPB, *supra* note 172, at 32.
204 Court of Justice of the European Union, C-434/16, Peter Nowak v Data Protection Commissioner, 20 December 2017. 轉引自 EDPB, *supra* note 172, at 31.
205 EDPB, *supra* note 172, at 33.

等運用之控管者，並因此受到懲戒或刑事訴訟或監管機關之行政處分。EDPB指出，依據GDPR第24條，採取適當措施為雇主責任之一，包括實施教育訓練到懲戒程序，以確保運用符合GDPR及不會發生資料侵害事件[206]。

2. 「正在被運用」的個人資料

針對正在運用之資料所進行的評估，應盡可能反映控管者收到請求時的情況，而回覆應涵蓋當時所有資料。這表示控管者必須試圖識別與當事人相關之所有資料運用作業，而不得無故遲延[207]。

3. 新近用請求

若控管者過去已完成近用請求，且該請求非屬過度請求，控管者不得限縮新請求之範圍。就同一當事人之任何進一步近用請求而言，控管者不應僅通知當事人自上次請求以來所運用之個人資料或運用本身之單純變更，除非當事人另有明示同意[208]。

(三) 關於運用及當事人權利之資訊

除對個人資料本身之近用，控管者必須依據GDPR第15條第1項第a款至第h款及第15條第1項，提供關於運用及當事人權利之資訊。大部分關於該等具體項目之資訊均已至少以一般形式完成彙編於GDPR第30條所定之控管者運用作業紀錄，及/或GDPR第12條至第14條所定之隱私權通知中。因此，第一步先查閱第29條工作小組之「第2016/679號規則下之透明化指引」，以瞭解依據GDPR第13條及第14條應提供之資訊內容可能會有所幫助[209]。

第 15 條第 1 項各款	**條文內容[210]**

[206] EDPB, *supra* note 172, at 34.
[207] EDPB, *supra* note 172, at 17.
[208] EDPB, *supra* note 172, at 35.
[209] EDPB, *supra* note 172, at 35-36.
[210] EDPB, *supra* note 172, at 36-39.

(a) 處理之目的	➢ 目的相關資訊應針對提出請求之當事人的實際情況具體說明確切運用目的。僅列出控管者之通用目的，而未就該當事人的屆時情況說明控管者的運用目的是不夠的。 ➢ 若控管者有多項運用目的，則必須說明哪些類別資料是為哪些目的所運用。 ➢ 透明運用原則要求以便利當事人查詢的方式向其提供運用法律依據之相關資訊。
(b) 個人資料所涉及之類型	➢ 若近用請求係依據 GDPR 第 15 條提出，則除了向請求人提供實際運用之資料外，亦必須說明於特定情況下運用的特定類別資料。
(c) 已揭露或將予揭露之資料接收方或資料接收方類型，尤其是在第三國境內或國際組織之資料接收方	➢ 所謂「接收方」，係指基於向自然人或法人、公務機關、機構或其他單位揭露個人資料。 （GDPR 第 4 條第 9 項）
(d) 如可能，個人資料將被儲存之預期期間，或如告知期間不可能者，確定該期間所採用之標準	➢ 控管者提供之資訊必須足夠精確，使當事人得以知悉其資料將繼續被保存多久。 ➢ 若無法說明刪除時間，則應說明保存期間及該等期間之起始或觸發事件（如合約之終止，保固期之屆滿等）。
(e) 向控管者請求更正、刪除、限制處理或拒	➢ 當事人有權向監管機關提出申訴（第 15 條第 1 項第 f 款）之相關資訊不會因具

絕處理與當事人相關個人資料之權利	體案件情況而有變更，而第 15 條第 1 項第 e 款所定當事人權利則會因運用之法律依據而有不同。
(f) 向監管機關提起申訴之權利	➢ 關於控管者依據第 12 條第 2 項促進當事人行使權利之義務，控管者對該等請求之回覆，應針對當事人個別情況及與其相關之運用作業進行調整。應避免提供不適用當事人具體情況的相關權利資訊。
(g) 個人資料非自當事人蒐集所得者，關於該來源之任何充分資訊	➢ 若個人資料並非自當事人處所蒐集，即必須提供關於資料來源之「任何可用資訊」。可用資訊之範圍可能會隨時間而有所變化。 ➢ 範例： 某一大公司之隱私權政策指出：「為進行信用調查，本公司會將您的姓名、地址及出生日期發送予以下服務供應商，例如：(1)金融資訊機構 X；(2)企業資訊供應商 Y；(3)商業信用資訊機構 Z。」若事前不清楚哪些公司將參與運用，則於隱私權政策中提供符合條件之公司名稱就足夠；若當事人依據第 15 條提出請求，除說明已取得信用資訊外，亦必須（事後）揭露哪些公司參與信用調查。若個人資料並非自當事人處蒐集，則資料運用資訊包括「任何關於其來源之可用資訊」。
(h) 存在第 22 條第 1 項及第 4 項所定自動化決策（包括建檔）	➢ 所有當事人均應有權以有意義的方式被告知自動化決策之存在及基本邏輯，包

者，至少在該等情況，為當事人之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。	括關於當事人之剖析，及此等運用的可能意義及預期結果。 ➢ 第 15 條第 1 項第 h 款所定資訊須更具體明確，說明對請求近用之當事人作出具體決策的理由。

依據GDPR第13條第1項第f款及第14條第1項第f款，必須提供關於擬向第三國或國際組織移轉資料之資訊，包括是否存在經歐盟執委會認定之適足性決定或適當之保護措施。惟就第15條所定之近用權請求而言，僅有在實際向第三國或國際組織進行移轉的情況下，始得提供其依據第46條實施適當保護措施之資訊[211]。

四、控管者如何提供近用？

當事人應有權近用其被控管者運用的所有資訊。舉例而言，這表示控管者有義務於其資訊科技（IT）系統及非資訊科技（non-IT）歸檔系統中搜尋個人資料。於進行該等搜尋時，控管者應依據資料架構，使用組織中可能會因此於系統中產生配對結果的當事人可用資訊。然而，控管者不得要求當事人提供超出識別當事人所必須之資訊[212]。因此，控管者應注意檢索資料的流程亦應以資料保護友善的方式設計，以避免損害他人（例如控管者的員工）隱私[213]。

(一) 採取「適當措施」

GDPR第12條第1項規定，控管者應採取適當措施，以簡明、透明、可理解及易近用之形式，採用清晰及簡明之語言，向當事人提供第15條關於運用之任何資訊。在決定哪些措施具適當性時，控管者必須考量到所有相關情況，包括但不限於正在運用的資料量、其資料運用之複雜性及其對當事人之瞭解，例如，特別是當事人為兒童、老人

[211] EDPB, *supra* note 172, at 39.
[212] EDPB, *supra* note 172, at 39.
[213] EDPB, *supra* note 172, at 40.

或殘疾人士的情況[214]。因此，適當措施會視個案而有所不同[215]。於進行評估時，應係依據各案件之具體情況，選擇最適當方法來提供此權利所涵蓋的所有資訊。大規模運用大量資料之控管者必須同意付出大量努力，以確保近用權得以簡明、透明、可理解及易近用之形式，透過簡明且清晰的語言向當事人提供[216]。

(二) 分層方法

與近用權相關之分層方法，係指控管者於特定情況下，得分層提供第15條所定個人資料及補充資訊。第一層應包括關於運用及當事人依據第15條第1項第a款至第h款及第15條第2項所享有權利之資訊，以及所運用個人資料之第一部分。第二層則應提供更多個人資料[217]。分層方法之使用並非適合所有控管者或所有情況，只有在當事人難以理解資訊之全部內容時，才應使用此等方法。控管者需要證明使用分層方法得為當事人增加價值，並得協助其理解所提供之資訊[218]。

(三) 格式

有關近用正在運用之個人資料，依據GDPR第15條第3項規定，若當事人以電子形式提出要求，除當事人另有說明，應以常用電子形式提供該資訊。常用電子形式的範圍，會隨著時間而有所變化，並應以當事人之合理期望為基礎，而非基於控管者於其日常運作中使用之格式，且不應要求當事人購買特定軟體來取得資訊近用[219]。此外，當事人取得的資訊應以可體現資訊且永久的形式（紙本、電子）呈現[220]。

(四) 提供近用的時間點

時限自控管者收到資料請求時起算，不管控管者事實上是否已

[214] EDPB, *supra* note 172, at 40-42.
[215] EDPB, *supra* note 172, at 40.
[216] EDPB, *supra* note 172, at 40-41.
[217] EDPB, *supra* note 172, at 44.
[218] EDPB, *supra* note 172, at 45.
[219] EDPB, *supra* note 172, at 45.
[220] EDPB, *supra* note 172, at 46.

注意到該請求。當控管者因不確定提出請求之人的身分而需要與當事人溝通時，得暫停該時間之計算，直到控管者自當事人處取得必要資訊為止，但前提為控管者已要求提供額外資訊，不得無故拖延[221]。如有必要，考量到請求之複雜性及數量，控管者得將對近用請求之回覆時間再延長兩個月。構成複雜請求的要件會依據各案件的具體情況而有所不同，須考量的因素可能涉及：控管者運用之資料量、資訊之保存方式、需要遮蔽資訊之情況，以及資訊是否需要進一步處理（使其可被理解）[222]。

五、近用權之限縮及限制

近用權受GDPR第15條第4項（他人之權利及自由）及GDPR第12條第5項（顯無理由或過度要求）所拘束。此外，歐盟或會員國法律得依據GDPR第23條限制近用權。為公共利益而就科學、歷史研究或統計目的或建檔目的所為之個人資料運用，可依據GDPR第89條第2項及第89條第3項限縮近用權，而就新聞目的或學術、藝術或文學表達目的所為之個人資料運用，則可依據GDPR第85條第2項限縮近用權[223]。

(一) 不影響他人權利及自由（GDPR第15.4條）

依據GDPR第15條第4項規定：「取得複製本之權利不得對他人之權利及自由產生不利影響」。近用權之行使，不應影響他人之權利或自由，包括營業秘密或智慧財產權，特別是保護軟體之著作權。於解釋GDPR第15條第4項時，必須特別注意不應無合理事由擴大GDPR第23條所定限制，該等限制僅有在嚴格條件下才能實施[224]。

「他人」係指除當事人以外之任何其他正在行使其近用權之人或實體。因此，控管者或受託運用者之權利及自由（例如營業秘密及智慧財產權）可能會被考量在內。若歐盟立法者想排除控管者或受託運用者之權利及自由，則會使用「第三人」一詞，而依據GDPR第4條

221 EDPB, *supra* note 172, at 47-48.
222 EDPB, *supra* note 172, at 48.
223 EDPB, *supra* note 172, at 49.
224 EDPB, *supra* note 172, at 49-50.

第10項定義之「第三人」，係指當事人、控管者、受託運用者及在控管者或受託運用者直接授權下被授權運用個人資料之人以外之自然人或法人、公務機關、機構或其他團體[225]。

(二) 無償提供原則（GDPR第12條第5項）

依據GDPR第12條第5項規定：「第13條及第14條所定應提供之資訊及第15條至第22條及第34條所定任何溝通及採取之任何行動，應無償提供之。如當事人之請求『明顯無理由』或『過度』者，尤其是基於該等請求過於重複者，控管者得：(a)考量所要求提供之資訊或溝通或採取行動之行政成本，收取適當費用；或(b)拒絕該請求。控管者應就該請求之明顯無理由或過度性負舉證責任[226]。」以下依據近用權指引對「明顯無理由」及「過度請求」之說明，分別進行討論：

1. 明顯無理由

若採用客觀方法判斷明顯不符合GDPR第15條規範，則近用權之請求即屬明顯無理由。就近用權之請求而言，適用第12條第5項「顯無理由」的情況非常有限。控管者不應因當事人先前提交過顯無理由或過度之請求，或若請求中包含不客觀或不恰當之語言，就推定請求屬顯無理由[227]。

2. 過度請求

GDPR並未提供「過度」一詞之定義，對「過度」之評估取決於控管者所進行的分析及其所處產業之具體情況[228]。控管者必須仔細

[225] GDPR art 4.10: 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
[226] GDPR art 12.5: 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. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
[227] EDPB, *supra* note 172, at 53.
[228] EDPB, *supra* note 172, at 53-54.

考量個別案件的特殊情況，例如雙方接觸頻率。因此，當事人得再次行使其近用權之「合理間隔」，依個案有所不同。控管者資料庫發生變更的頻率越高，當事人得被允許請求近用的頻率就越高，而不會被認定為過度。在判斷合理時間間隔是否已終了時，控管者應依據當事人的合理期望來考量：

- 資料變更之頻率－資訊於兩次請求之間是否變更的可能；
- 資料之性質－包括其是否為特別敏感資料；
- 運用之目的－包括若揭露運用過程是否可能對請求人造成損害（傷害）；及
- 後續請求是否涉及同一類型之資訊或運用[229]。

此外，近用權指引針對「非過度請求」及「過度請求」的狀況，提出以下敘述及舉例：

非過度請求	過度請求
➢ 當事人並未就其請求提出原因，或控管者認為此請求沒有意義； ➢ 當事人使用不恰當或不禮貌的語言；以及， ➢ 當事人擬利用該等資料向控管者提出進一步主張[230]。	➢ 當事人提出請求的同時表示願意撤回請求以換取控管者提供某種形式之利益；或 ➢ 該請求為惡意用來騷擾控管者或其員工者，除造成干擾外並無其他目的；例如基於以下事實所提請求： ✓ 當事人於請求本身或其他通訊中明確表示其意圖是造成破壞，除此之外無其他意圖；或 ✓ 當事人有系統地向控管者發送不同請求作為某活動之一部分，例如每週一次，其目的及效果是造成干擾[231]。

[229] EDPB, *supra* note 172, at 54.
[230] EDPB, *supra* note 172, at 56.
[231] EDPB, *supra* note 172, at 56.

依據第12條第4項，若控管者拒絕對近用請求之全部或一部採取行動，其必須至遲於收到請求後一個月內將下列資訊通知當事人，不得無故遲延，包括：(1)拒絕之原因、(2)向監管機關提出申訴之權利、(3)尋求司法救濟之可能性[232]。此外，依據GDPR第12條至第22條，若無合理事由即拒絕近用權之請求，將被視為對當事人權利之侵害，權責監管機關得依據GDPR第83條第5項第b款處以行政罰鍰。若當事人認為其當事人權利受到侵害，則有權依據GDPR第77條提出申訴[233]。

第三節 與我國個人資料保護法之重點比較

一、 我國個人資料保護法針對當事人近用權之規範

我國個人資料保護法有關於當事人近用權之規定，主要規定於個人資料保護法第3條及第10條，前者規定「當事人的權利種類[234]」，後者規定「公務機關或非公務機關得拒絕當事人請求查詢個人資料、提供閱覽或製給複製本之事由[235]」。自電腦處理個人資料保護法第4條（即個人資料保護法第3條，修法時僅作條次變更及文字酌修）之立法理由可知，本條規定係為保護「當事人之人格權益」，為充分保護起見，故明定不得預先拋棄或以特約限制之。

自我國個人資料保護法第1條[236]及電腦處理個人資料保護法第1條立法理由[237]觀之，我國對個人資料保護係以保障人格權免受侵害

---

232 EDPB, *supra* note 172, at 56-57.

233 EDPB, *supra* note 172, at 57.

234 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」

235 個人資料保護法第 10 條：「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」

236 個人資料保護法第 1 條：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」。

237 電腦處理個人資料保護法第 1 條立法理由：「電腦科技進步迅速，使電腦能大量、快速處理各類資料，且運用日趨普及，因而對國民經濟之提昇有重大貢獻。惟個人資料因濫用電腦而侵害當事人權益之情形日漸嚴重，亦引起民主先進國家之關切。故經濟合作暨發展組織（OECD）

為目的，並曾參考經濟合作暨發展組織（OECD）及歐盟相關規定。對於當事人的近用權，我國憲法並未如《歐盟基本權利憲章》一般，明定當事人的權利；而將近用權引自隱私權，將人民對個人資料使用的權利視為隱私權的一環[238]。惟必須注意者，大法官於釋字第603號解釋文中亦指出：「憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第23條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」由此可知，在我國法下資訊隱私權及作為其權利內涵之一的近用權，皆非絕對不可侵犯的權利。

二、 GDPR、指引文件與我國法之不同

(一) 當事人向控管者請求的資料種類及範圍

我國個人資料保護法及GDPR皆有針對當事人得向控管者請求個人資料的權利。我國對於個人資料的定義，係定於個人資料保護法第2條第1款：「個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」而GDPR第4條亦定義所謂「個人資料」，係指有關識別或可得識別自然人（「個人資料當事人」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基

於一九八〇年九月通過管理保護個人隱私及跨國界流通個人資料之指導綱領，歐洲理事會亦於一九八一年完成保護個人資料自動化處理公約，並提出八項原則以供遵守。迄今已有瑞典、美國、紐西蘭、德國、法國、丹麥、挪威、奧地利、盧森堡、冰島、加拿大、英國、芬蘭、愛爾蘭、澳洲、日本、荷蘭等十七國制定相關法律以保護個人資料。」

[238] 依據大法官釋字第 603 號解釋文：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」

因、心理、經濟、文化或社會認同等具體因素之識別工具[239]。自上述個人資料的定義觀之，個人資料保護法與GDPR純就條文上對個人資料的定義較為接近，皆是從以「是否能識別出自然人」為核心。就我國當初制定個人資料保護法第2條的立法理由觀之，本條個人資料之定義，亦係參考歐盟資料保護指令、日本、德國及英國法之立法例。

實務上，曾有當事人為查其個人前科紀錄，向臺灣高等法院請求製給前案紀錄表複製本。雖經臺灣高等法院函覆，以「臺灣高等法院全國前案紀錄系統查詢作業規範」駁回申請。惟經當事人向司法院進行訴願，訴願決定認為「臺灣高等法院全國前案紀錄系統查詢作業規範」，性質上係屬行政程序法第159條規定之行政規則[240]，不能牴觸法律之規定或增加法律所無之限制。當事人係依個人資料保護法第3條規定，就其個人之前案資料請求製給複製本，除符合法定例外情形，臺灣高等法院不得拒絕製給複製本[241]。

依據我國個人資料保護法第3條規定，當事人能向控管者行使近用權之標的，僅限於「個人資料[242]」。而依據GDPR第15條規定，當事人除了能請求接近使用個人資料外，依據近用權指引之說明，尚能請求其他資訊，如個人資料將被儲存之預期期間[243]，或如涉及自動化

---

[239] GDPR art 4.1: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[240] 行政程序法第 159 條：「（第一項）本法所稱行政規則，係指上級機關對下級機關，或長官對屬官，依其權限或職權為規範機關內部秩序及運作，所為非直接對外發生法規範效力之一般、抽象之規定。（第二項）行政規則包括下列各款之規定：一、關於機關內部之組織、事務之分配、業務處理方式、人事管理等一般性規定。二、為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。」。

[241] 參司法院訴願決定書 105 年訴字第 26 號。

[242] 個人資料保護法第 3 條：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之……」

[243] GDPR art 5.1: The data subject shall have the 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 and the following information:…(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period…

決策之邏輯性有意義之資訊或重要性與預設結果[244]。有關其他資訊之定義，詳見近用權指引第110至120段之說明[245]。

(二) 提供資料的程序

我國在近用權的規定上，僅有原則上的規範，對於如何判斷及如何提供當事人資料，並未如GDPR有詳細的規範。近用權指引除了上述摘要的內容外，於近用權指引最末三頁，亦提供控管者接到當事人為行使其近用權之請求，應如何作為的判斷流程圖，讓控管者在當事人提出請求時，對該請求進行判斷[246]。本文以下製作簡要版的流程圖，敬供讀者卓參：

步驟		內容
步驟一	確認當事人之請求	➢ 確認請求之標的範圍 ➢ 確認請求人及請求標的之關係
步驟二	控管者如何回應當事人之請求	➢ 採取適當的回應措施：簡明、透明、可理解、易於近用 （GDPR 第 12 條第 1 項及第 2 項） ➢ 採用分層方式 ➢ 不得無故延遲，至遲 1 個月內（於特殊情況下可延展 2 個月） （GDPR 第 12 條第 3 項）
步驟三	確認是否可以拒絕當事人之請求	➢ 是否影響他人之權利及自由 （GDPR 第 15 條第 4 項） ➢ 是否明顯無理由或有過度請求的情形 （GDPR 第 12 條第 5 項）

[244] GDPR art 5.1: (h) 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.…

[245] EDPB, *supra* note 172, at 35-39.

[246] EDPB, *supra* note 172, at 58-60.

(三) 權利行使的界限

我國個人資料保護法將資訊近用權的界限規範於個人資料保護法第10條，依據該條規定，僅有基於公益、法定職務以及涉及蒐集機關或第三人之重大利益時，方能拒絕當事人查詢、提供閱覽或製給複製本之請求[247]。依據個人資料保護法施行細則第18條之規定，所謂「妨害第三人之重大利益」，係指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

雖然GDPR第15條第4項亦僅規定：「第3項所定取得副本之權利不應影響其他人之權利及自由[248]。」，針對當事人近用權及他人權利及自由的權衡，近用權指引說明，應依據「比例原則」（the principle of proportionality）進行判斷[249]。此外，近用權指引於第171段亦說明，即便是為了不影響他人之權利及自由，控管者仍不能拒絕提供當事人所有的資料，並要盡力找到可能的兩全方式[250]。

有關個人資料保護法第10條但書所稱「重大利益」相關之判決，僅有少數判決討論到有關當事人權利與他人權利權衡的爭議[251]。近用權指引提供以下三個案例，在我國欠缺前例的情形下，似可作為參考：[252]

案例一（涉及他人權利）

客戶擬取得其與零售商客服人員之錄音複製本。零售商首先就此請求進行分析，發現該對話包含之個人資料亦與他人（即客服人員）相關。其次，為評估提供複製本是否會影響他人（即客服人員）之

[247] 個人資料保護法第 10 條：「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益。」。

[248] GDPR art 15.4: The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

[249] EDPB, *supra* note 172, at 50.

[250] EDPB, *supra* note 172, at 50-51.

[251] 參臺北高等行政法院 106 年度訴字第 865 號判決。

[252] EDPB, *supra* note 172, at 50-52.

權利及自由，則零售商必須平衡相互衝突之利益，特別是考量到客服人員之權利及自由可能面臨風險之可能性及重大性，該等風險存在於向客戶提供錄音的過程中。若錄音中與客服人員相關的個人資料非常有限，(1)只有該客服人員的聲音，該客服人員不容易被識別，(2)討論的內容屬專業性質，且(3)當事人是對話者。基於上述情況，控管者客觀得出結論，近用權之行使不會對客服人員之權利及自由產生不利影響，因此，控管者得向當事人提供完整錄音，包括與客服人員相關之部分[253]。

案例二（涉及營業秘密）

醫療用品商店之客戶向醫療用品商店依據GDPR第15條請求腿部測量結果之資料。醫療用品商店依據第15條第4項規定拒絕當事人，醫療用品商店主張腿部測量結果係以其特殊、精確之測量技術所測得，測量結果屬受保護之營業秘密。此時，控管者應證明以下兩點，方得適用第15條第4項：第一，若不透露測量的執行方式，就無法向當事人提供關於測量結果之資訊；及第二，執行測量方式之資訊（包括相關測量點之確切位置）屬營業秘密。然而，控管者仍須提供任何不會揭露其營業秘密之測量結果資訊，即使控管者因此需耗費心力變更及編輯測量結果[254]。

案例三（涉及營業秘密）

玩家X為遊戲平台Y上之使用者，玩家X因其無法再登入帳戶，向控管者請求與其相關之所有個人資料及其帳戶被限制之原因。平台Y應向玩家X提供運用玩家X個人資料之複製本，並向玩家X確認，因為玩家X使用一項或多項違反一般使用條款之遊戲作弊行為，平台Y決定限制玩家X使用其帳戶。惟只要反作弊軟體技術作

[253] EDPB, *supra* note 172, at 51.
[254] EDPB, *supra* note 172, at 51-52.

業之任何部分被視為營業秘密，則平台Y無義務揭露該資料，即使該資訊與玩家X有關亦然。由於揭露反作弊軟體技術之操作，將可能令使用者規避偵測，是以，平台Y之營業秘密排除對該等個人資料之揭露[255]。

此外，我國個人資料保護法第14條雖規定：「查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。」；而對照GDPR第12條第5項規定：若是當事人之請求明顯無理由或是過度，尤其是重複之請求，控管者得考量所要求資料或行為的成本，收取適當費用，或是拒絕該請求；惟控管者應舉證證明該請求明顯無理由或過度[256]。相較我國個人資料保護法，GDPR針對是否要支付費用取得資料，提供了兩個判斷要素：明顯無理由或是過度，以避免當事人過當的請求，影響控管者日常的業務[257]。本文以為，我國似可參考GDPR第12條第5項規定，訂定界線。

第四節 小結

綜上所述，我國目前對於當事人之近用權，雖已於個人資料保護法有相關規定，但仍有諸多未竟之處。現行規範在實際操作上，欠缺細節性規定及相關案例，我國公務機關或非公務機關在適用個人資料保護法第3條時，不免有對於提供資料的範圍、方式及界線各自為政的情形。在對個人資料保護法適用時，不一致的解釋，將可能造成不慎侵害當事人權利之疑慮。本文以為，法制的發展必須仰賴經驗及案例的累積，尋找最適合我國的制度，在我國尚未有相關法規或主管機關函釋針對當事人近用權有執行上的細節規範前，建議主管機關本於職權，審酌其他外國法例所揭示的相

[255] EDPB, *supra* note 172, at 52.
[256] GDPR art 12.5: 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. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
[257] EDPB, *supra* note 172, at 53-56.

關作法，給予我國公務機關及非公務機關相關在執行上的建議。

我國個人資料保護法在制定及修訂時，多有參考GDPR前身歐盟資料保護指令之規定，本文參考GDPR及近用權指引文件的規範設計架構，認為我國主管機關或可參酌歐盟法的規範模式，在保護當事人權利的同時，亦考量控管者如何面對當事人大量請求時的因應措施。本文有以下幾個建議做法：

一、透過修法程序，參考GDPR及近用權指引的規定，健全當事人近用權相關規定。例如：增訂如GDPR第15條第2項國際傳輸前，賦予當事人受通知該傳輸有適當保護措施的規定[258]。

二、建議統一解釋個人資料保護法的主管機關，對個人資料保護法原則性的規定，進行通案的解釋，並發布類似於近用權指引之文件，以避免不同目的事業主管機關及不同事業間可能產生規範歧異的問題。

三、近用權指引於最末三頁，提供控管者在遇到當事人請求時，如何判斷資料屬性、如何提供資料以及確認是否有不需要提供資料事由的流程確認表。本文以為，礙於我國立法制度較耗時，在法規修正前，我國主管機關可以參考此流程表，制定符合我國行政程序的公務機關內部申請流程。在公務機關建立該流程表後，亦可作為民間控管者遇到相關當事人行使近用權的參考[259]。

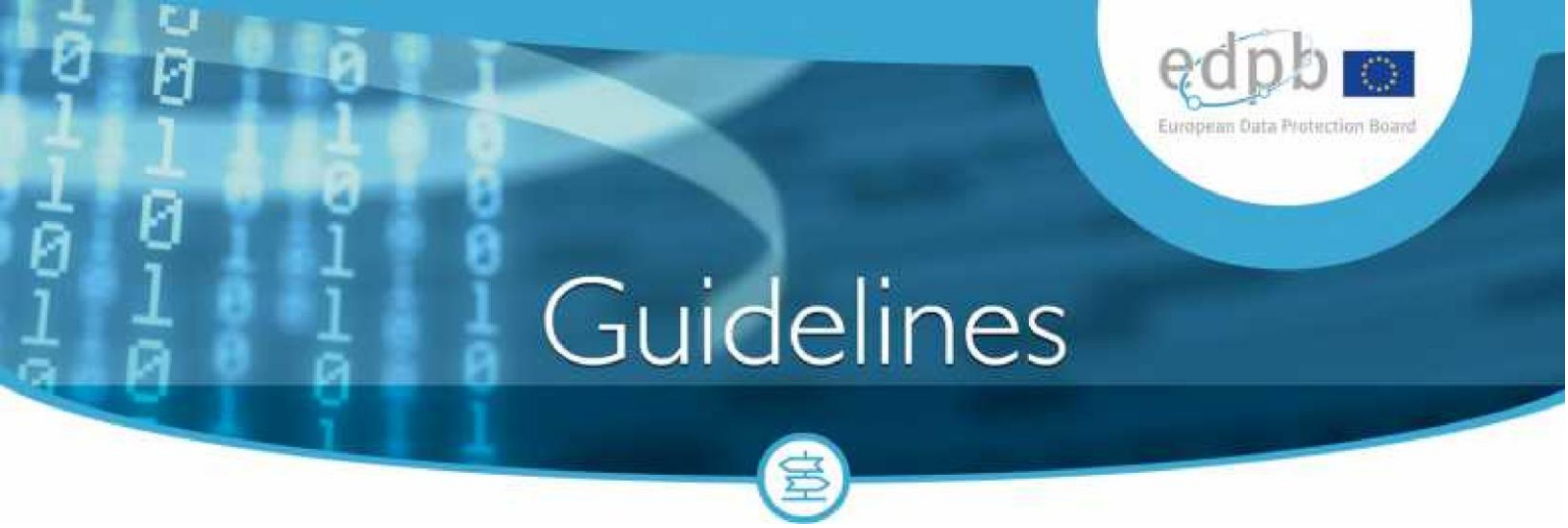
四、考量每個行業所涉及個人資料及其他資訊蒐集、處理及利用的程度與密度不同，主管機關雖然可參考GDPR及近用權指引相關內容，透過修法或是發布函釋制定一套較為周全的制度。本文以為，法規及函釋等法規範都僅是最低標準，政府除以法規範硬性要求符合個人資料保護法，也可以用宣導及獎勵的方式，向公務機關及非公務機關宣導自行按照按更高標準的GDPR，以完善符合該產業資料屬性的申請制度，

[258] GDPR art 15.2: Where personal data are transferred to the third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
[259] EDPB, *supra* note 172, at 58-60.

一則得以增進服務品質，降低資料提供者的疑慮，完善對當事人的人格權保障；二則周延的資料管理制度可以降低資料洩漏的風險（特別是針對已蒐集到的個人資料，後續如何保存及提供當事人參考）；三則對非公務機關來說，在有機會進軍外國時，能降低法遵成本，更有效率地符合當地法規。

第五章 指引翻譯

詳如後附。



Guidelines 01/2021 on Examples regarding Personal Data Breach Notification

個人資料侵害事件通報範例指引 01/2021

Adopted on 14 December 2021
2021 年 12 月 14 日通過

Version 2.0
第 2.0 版

Version history
版本歷程

Version 2.0 第 2.0 版	2021 年 12 月 14 日	Adoption of the Guidelines after public consultation 經徵詢公眾意見後通過本指引。
Version 1.0 第 1.0 版	2021 年 1 月 14 日	Adoption of the Guidelines for public consultation 經徵詢公眾意見通過本指引。

Table of contents
目錄

1. INTRODUCTION 導言 7

2. RANSOMWARE 勒索軟體 13

2.1.CASE NO. 01: RANSOMWARE WITH PROPER BACKUP AND WITHOUT EXFILTRATION 案例 01：勒索軟體攻擊－有適當備份且未發生資料外洩的情況 13

2.1.1.CASE NO. 01 - PRIOR MEASURES AND RISK ASSESSMENT 案例 01－事前措施及風險評估 15

2.1.2.CASE NO. 01 – MITIGATION AND OBLIGATIONS 案例 01－緩解措施及義務 17

2.2.CASE NO. 02: RANSOMWARE WITHOUT PROPER BACKUP 案例 02：勒索軟體攻擊－無適當備份之情況 18

2.2.1.CASE NO. 02 - PRIOR MEASURES AND RISK ASSESSMENT 案例 02－事前措施及風險評估 19

2.2.2.CASE NO. 02 – MITIGATION AND OBLIGATIONS 案例 02－緩解措施及義務 21

2.3.CASE NO. 03: RANSOMWARE WITH BACKUP AND WITHOUT EXFILTRATION IN A HOSPITAL 案例 03：勒索軟體－發生在醫療院所、有備份且未發生資料外洩之情況 22

2.3.1.CASE NO. 03 - PRIOR MEASURES AND RISK ASSESSMENT 案例 03－事前措施及風險評估 23

2.3.2.CASE NO. 03 – MITIGATION AND OBLIGATIONS 案例 03－緩解措施及義務 24

2.4.CASE NO. 04: RANSOMWARE WITHOUT BACKUP AND WITH EXFILTRATION 案例 04：勒索軟體攻擊－無備份且有發生資料外洩之情況 25

2.4.1.CASE NO. 04 - PRIOR MEASURES AND RISK ASSESSMENT 案例 04－事前措施及風險評估 25

2.4.2.CASE NO. 04 – MITIGATION AND OBLIGATIONS 案例 04－緩解措施及義務 27

2.5.ORGANIZATIONAL AND TECHNICAL MEASURES FOR PREVENTING / MITIGATING THE IMPACTS OF RANSOMWARE ATTACKS 防範勒索軟體攻擊/緩解其影響之組織上及技術上措施 28
3. DATA EXFILTRATION ATTACKS 資料外洩攻擊 30
3.1.CASE NO. 05: EXFILTRATION OF JOB APPLICATION DATA FROM A WEBSITE 案例 05：網站之求職資料外洩 31
3.1.1.CASE NO. 05 - PRIOR MEASURES AND RISK ASSESSMENT 案例 05－事前措施及風險評估 31
3.1.2.CASE NO. 05 – MITIGATION AND OBLIGATIONS 案例 05－緩解措施及義務 33
3.2.CASE NO. 06: EXFILTRATION OF HASHED PASSWORD FROM A WEBSITE 案例 06：網站之雜湊密碼外洩 34
3.2.1.CASE NO. 06 - PRIOR MEASURES AND RISK ASSESSMENT 案例 06－事前措施及風險評估 34
3.2.2.CASE NO. 06 – MITIGATION AND OBLIGATIONS 案例 06－緩解措施及義務 35
3.3.CASE NO. 07: CREDENTIAL STUFFING ATTACK ON A BANKING WEBSITE 案例 07：銀行網站遭憑證填充攻擊 36
3.3.1.CASE NO. 07 - PRIOR MEASURES AND RISK ASSESSMENT 案例 07－事前措施及風險評估 37
3.3.2.CASE NO. 07 – MITIGATION AND OBLIGATIONS 案例 07－緩解措施及義務 38
3.4.ORGANIZATIONAL AND TECHNICAL MEASURES FOR PREVENTING / MITIGATING THE IMPACTS OF HACKER ATTACKS 防範駭客攻擊/緩解其影響之組織上及技術上措施 39
4. INTERNAL HUMAN RISK SOURCE 內部人為風險來源 41
4.1.CASE NO. 08: EXFILTRATION OF BUSINESS DATA BY AN EMPLOYEE 案例 08：員工洩漏業務資料 41
4.1.1.CASE NO. 08 - PRIOR MEASURES AND RISK ASSESSMENT 案例 08－事前措施及風險評估 42
4.1.2.CASE NO. 08 – MITIGATION AND OBLIGATIONS 案例 08－緩解措施及義務 43

4.2.CASE NO. 09: ACCIDENTAL TRANSMISSION OF DATA TO A TRUSTED THIRD PARTY 案例 09：意外將資料傳輸予可信賴之第三方 44
4.2.1.CASE NO. 09 – PRIOR MEASURES AND RISK ASSESSMENT 案例 09－事前措施及風險評估 45
4.2.2.CASE NO. 09 – MITIGATION AND OBLIGATIONS 案例 09－緩解措施及義務 46
4.3.ORGANIZATIONAL AND TECHNICAL MEASURES FOR PREVENTING / MITIGATING THE IMPACTS OF INTERNAL HUMAN RISK SOURCES 防範內部人為風險來源/緩解其影響之組織上及技術上措施 47
5. LOST OR STOLEN DEVICES AND PAPER DOCUMENTS 滅失或遭竊之裝置及紙本文件 49
5.1.CASE NO. 10: STOLEN MATERIAL STORING ENCRYPTED PERSONAL DATA 案例 10：存有經加密個人資料之裝置遭竊 49
5.1.1.CASE NO. 10 - PRIOR MEASURES AND RISK ASSESSMENT 案例 10－事前措施及風險評估 50
5.1.2.CASE NO. 10 – MITIGATION AND OBLIGATIONS 案例 10－緩解措施及義務 50
5.2.CASE NO. 11: STOLEN MATERIAL STORING NON-ENCRYPTED PERSONAL DATA 案例 11：存有未加密個人資料之裝置遭竊 51
5.2.1.CASE NO. 11 - PRIOR MEASURES AND RISK ASSESSMENT 案例 11－事前措施及風險評估 51
5.2.2.CASE NO. 11 – MITIGATION AND OBLIGATIONS 案例 11－緩解措施及義務 52
5.3.CASE NO. 12: STOLEN PAPER FILES WITH SENSITIVE DATA 案例 12：含有敏感性資料之紙本文件遭竊 53
5.3.1.CASE NO. 12 – PRIOR MEASURES AND RISK ASSESSMENT 案例 12－事前措施及風險評估 53
5.3.2.CASE NO. 12 – MITIGATION AND OBLIGATIONS 案例 12－緩解措施及義務 54
5.4.ORGANIZATIONAL AND TECHNICAL MEASURES FOR PREVENTING / MITIGATING THE IMPACTS OF LOSS OR THEFT OF DEVICES 防範裝置滅失或遭竊/緩解其影響之組織上及技術上措施 55
6. MISPOSTAL 郵遞錯誤 57

6.1.CASE NO. 13: POSTAL MAIL MISTAKE 案例 13：郵遞錯誤 57
6.1.1.CASE NO. 13 - PRIOR MEASURES AND RISK ASSESSMENT 案例 13－事前措施及風險評估 57
6.1.2.CASE NO. 13 – MITIGATION AND OBLIGATIONS 案例 13－緩解措施及義務 58
6.2.CASE NO. 14: HIGHLY CONFIDENTIAL PERSONAL DATA SENT BY MAIL BY MISTAKE 案例 14：高度機密之個人資料遭誤寄 58
6.2.1.CASE NO. 14 - PRIOR MEASURES AND RISK ASSESSMENT 案例 14－事前措施及風險評估 59
6.2.2.CASE NO. 14 – MITIGATION AND OBLIGATIONS 案例 14－緩解措施及義務 59
6.3.CASE NO. 15: PERSONAL DATA SENT BY MAIL BY MISTAKE 案例 15：個人資料遭誤寄 60
6.3.1.CASE NO. 15 - PRIOR MEASURES AND RISK ASSESSMENT 案例 15－事前措施及風險評估 60
6.3.2.CASE NO. 15 – MITIGATION AND OBLIGATIONS 案例 15－緩解措施及義務 61
6.4.CASE NO. 16: POSTAL MAIL MISTAKE 案例 16：郵遞錯誤 62
6.4.1.CASE NO. 16 - PRIOR MEASURES AND RISK ASSESSMENT 案例 16－事前措施及風險評估 62
6.4.2.CASE NO. 16 – MITIGATION AND OBLIGATIONS 案例 16－緩解措施及義務 63
6.5.ORGANIZATIONAL AND TECHNICAL MEASURES FOR PREVENTING / MITIGATING THE IMPACTS OF MISPOSTAL 防範郵遞錯誤/緩解其影響之組織上及技術上措施 63
7. OTHER CASES – SOCIAL ENGINEERING 其他案例－社交工程 65
7.1.CASE NO. 17: IDENTITY THEFT 案例 17：身分冒用 65
7.1.1.CASE NO. 17 - RISK ASSESSMENT, MITIGATION AND OBLIGATIONS 案例 17－風險評估、緩解及義務 66
7.2.CASE NO. 18: EMAIL EXFILTRATION 案例 18：電子郵件外洩 67
7.2.1.CASENO. 18 - RISK ASSESSMENT, MITIGATION AND OBLIGATIONS 案例 18－風險評估、緩解及義務 68

THE EUROPEAN DATA PROTECTION BOARD
歐盟個人資料保護委員會

Having regard to Article 70 (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, (hereinafter "GDPR"),
依據歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過保護自然人關於個人資料運用*和自由流通的 2016/679/EU 規則第 70(1e)條規定，並廢除第 95/46/EC 號指令下稱「GDPR」）；

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA Joint Committee No 154/2018 of 6 July 2018[1],
依據歐洲經濟區聯合委員會 2018 年 7 月 6 日第 154/2018 號決定修正的歐洲經濟區合約，特別是其附件 11 及第 37 號議定書[1]；

Having regard to Article 12 and Article 22 of its Rules of Procedure,
依據其議事規則第 12 條及第 22 條；且

Having regard to the Communication from the Commission to the European Parliament and the Council titled Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation[2],
經考量歐盟執委會向歐洲議會及歐盟理事會提交題為「資料保護作為公民賦權之支柱及歐盟對數位轉型之態度」—《一般資料保護規則》實施兩週年後」之公報[2]；

HAS ADOPTED THE FOLLOWING GUIDELINES
通過以下指引

1. INTRODUCTION
導言

1. The GDPR introduces, in certain cases, the requirement for a personal data breach

---

* 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」。

1 References to "Member States" made throughout this document should be understood as references to "EEA Member States".
本文件所稱「會員國」係指「歐洲經濟區會員國」。

2 COM(2020) 264 final, 24 June 2020.
2020 年 6 月 24 日第 COM(2020) 264 號公報（定稿版）。

to be notified to the competent national supervisory authority (hereinafter "SA") and to communicate the breach to the individuals whose personal data have been affected by the breach (Articles 33 and 34).
GDPR 規定於特定情況下，個人資料侵害事件必須向具管轄權之國家監管機關（下稱「監管機關」）通報，並將該個人資料侵害事件通知其個人資料受到影響之當事人（第 33 條及第 34 條）。

2. The Article 29 Working Party already produced a *general* guidance on data breach notification in October 2017, analysing the relevant Sections of the GDPR (Guidelines on Personal data breach notification under Regulation 2016/679, WP 250) (hereinafter "Guidelines WP250)[3]. However, due to its nature and timing, this guideline did not address all practical issues in sufficient detail. Therefore, the need has arisen for a *practice-oriented*, *case-based* guidance, that utilizes the experiences gained by SAs since the GDPR is applicable.
第 29 條工作小組業已於 2017 年 10 月編制一份關於個人資料侵害事件通報之一般性指引，分析 GDPR 相關條文（第 2016/679 號規則下之個人資料侵害事件通報指引，編號 WP250）（下稱「第 WP250 號指引」）[3]。然而，由於其性質及作成之時點，第 WP250 號指引並未就所有實務議題提供詳細說明，因此，實有必要匯集監管機關自 GDPR 實施以來所累積的經驗，編制一份以實務為導向且以案例為基礎之指引。

3. This document is intended to complement the Guidelines WP 250 and it reflects the common experiences of the SAs of the EEA since the GDPR became applicable. Its aim is to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment.
本文件旨在補充第 WP250 號指引，其集結歐洲經濟區內監管機關自 GDPR 實施以來所累積的共同經驗，以協助資料控管者決定如何處理個人資料侵害事件，及風險評估時該考量哪些因素。

4. As part of any attempt to address a breach the controller and processor should first be able to recognize one. The GDPR defines a "personal data breach" in Article 4(12) as "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".
控管者及受託運用者在試圖處理個人資料侵害事件時，首要之務即為識別個人資料侵害事件。GDPR 於第 4 條第 12 項中將「個人資料侵害事件」定義為「導致經傳輸、儲存或以其他方式運用之個人資料遭意外或非法破壞、

---

3 G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 endorsed by the EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
第 29 條工作小組第 WP250 號指引，修訂一版，2018 年 2 月 6 日，經歐盟個人資料保護委員會認可，第 2016/679 號規則下之個資侵害事件通知指引：https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052。

滅失、竄改、未經授權揭露或存取之安全性漏洞」。

5. In its Opinion 03/2014 on breach notification[4] and in its Guidelines WP 250, WP29 explained that breaches can be categorised according to the following three well-known information security principles:
第 29 條工作小組於其第 03/2014 號有關個人資料侵害事件通報[4]之意見書及第 WP250 號指引中說明，個人資料侵害事件可依據下列三項公認之資料安全性原則進行分類：

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
「機密性」侵害事件－個人資料遭未經授權或意外之揭露或存取。

- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
「完整性」侵害事件－個人資料遭未經授權或意外之竄改。

- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.[5]
「可用性」侵害事件－個人資料本身或其存取途徑遭未經授權或意外之滅失或破壞[5]。

6. 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. One of the most important obligation of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them.
個人資料侵害事件可能會對當事人造成許多重大不利影響，可能導致人身、財物或非財物損害，GDPR 說明該等影響包括：當事人喪失對其個人資料

---

4 G29 WP213, 25 March 2014, Opinion 03/2014 on Personal Data Breach Notification, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.
第 29 條工作小組第 WP213 號指引，2014 年 3 月 25 日，第 03/2014 號有關個資侵害事件通知之意見書，第 5 頁：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4。

5 See Guidelines WP 250, p. 7. - It must be taken into consideration that a data breach can concern either one category or more categories simultaneously or combined.
請參考第 WP250 號指引，第 7 頁。－應考量個資侵害事件可能涉及單一類別、多類別或不同類別組合之侵害事件。

之控制權、其權利受到限制、歧視、身分冒用或詐欺、財務損失、假名化遭到未經授權之逆轉、名譽損害，以及受到職業保密義務保護的個人資料之機密性遭破壞，亦包含該等當事人在經濟或社會方面所遭受的任何其他重大不利益。資料控管者最重要的義務之一，是評估當事人之權利及自由所面臨的風險，並實施適當之技術上及組織上措施來緩解該等風險。

7. Accordingly, the GDPR requires the controller to:
因此，GDPR 要求控管者：

- document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken[6];
記錄任何個人資料侵害事件，包括與個人資料侵害事件相關之事實、其影響及已採取之改正措施[6]；

- notify the personal data breach to the supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons[7];
將個人資料侵害事件通報監管機關，除非該個人資料侵害事件不太可能對自然人之權利及自由造成風險[7]；

- communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons[8].
當個人資料侵害事件可能導致自然人之權利及自由面臨高風險時，應將個人資料侵害事件通知當事人[8]。

8. Data breaches are problems in and of themselves, but they may be also symptoms of a vulnerable, possibly outdated data security regime, they may also indicate system weaknesses to be addressed. As a general truth, it is always better to prevent data breaches by preparing in advance, since several consequences of them are by nature irreversible. Before a controller can *fully* assess the risk arising from a breach caused by some form of attack, the root cause of the issue should be identified, in order to identify whether any vulnerabilities that gave rise to the incident are still present, and are still therefore exploitable. In many cases the controller is able to identify that the incident is likely to result in a risk, and is therefore to be notified. In other cases the notification does not need to be postponed until the risk and impact surrounding the breach has been fully assessed,

---

6 GDPR Article 33(5).
GDPR 第 33 條第 5 項。

7 GDPR Article 33(1).
GDPR 第 33 條第 1 項。

8 GDPR Article 34(1).
GDPR 第 34 條第 1 項。

since the full risk assessment can happen in parallel to notification, and the information thus gained may be provided to the SA in phases without undue further delay[9].

雖然個人資料侵害事件本身就是問題，但它也可能是資料安全系統有漏洞或需要更新時會發生的症狀，也可能反映出有需要處理的系統缺陷。一般而言，最理想的狀況是透過事前防範措施來避免個人資料侵害事件的發生，因為個人資料侵害事件的許多後果在本質上無法逆轉。在針對特定形式攻擊所造成的個人資料侵害事件進行完整風險評估前，控管者應先確認問題的根本原因，以確認引起該事故的任何漏洞是否仍然存在、且因此仍有可能遭到利用。在有些情況下，控管者能夠先確定該事故是否會導致風險，再視情況進行通報；但在其他情況下，為避免無故遲延，在該事件之風險及影響評估完成前，即應通報監管機關，後續再將評估中所取得的資訊分批提交予監管機關[9]。

9. The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.

當控管者認為該個人資料侵害事件可能對當事人之權利及自由造成風險時，就應該進行通報；控管者應於知悉個人資料侵害事件時即進行評估，不應等到詳細鑑識或實施（早期）緩解措施後，才評估該個人資料侵害事件是否可能導致風險（及是否應進行通報）。

10. If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the competent SA can use its corrective powers and may resolve to sanctions.

若控管者自行評估結果認為不太可能造成風險，但後續卻發現風險確實存在，權責監管機關可行使其公權力要求採取改正措施，並得作成相關處分。

11. Every controller and processor should have plans, procedures in place for handling eventual data breaches. Organisations should have clear reporting lines and persons responsible for certain aspects of the recovery process.

各控管者及受託運用者均應制訂計畫及程序來處理無法避免的個人資料侵害事件。組織應建立明確的通報架構，並就還原流程之特定環節指派負責人。

12. Training and awareness on data protection issues for the staff of the controller and processor focusing on personal data breach management (identification of a

---

9 GDPR Article 33(4).
GDPR 第 33 條第 4 項。

personal data breach incident and further actions to be taken, etc.) is also essential for the controllers and processors. This training should be regularly repeated, depending on the type of the processing activity and size of the controller, addressing latest trends and alerts coming from cyberattacks or other security incidents.
控管者及受託運用者務必為其人員提供資料保護議題之教育訓練及宣導，著重於個人資料侵害事件管理（識別個人資料侵害事故及應採取的後續措施等）。該等教育訓練視資料運用活動之類型及控管者之規模而定，應定期重複辦理，以瞭解網路攻擊或其他安全事故之最新趨勢及警訊。

13. The principle of accountability and the concept of data protection by design could incorporate analysis that feeds into a data controller's and data processor's own "Handbook on Handling Personal Data Breach" that aims to establish facts for each facet of the processing at each major stage of the operation. Such a handbook prepared in advance would provide a much quicker source of information to allow data controllers and data processors to mitigate the risks and meet the obligations without undue delay. This would ensure that if a personal data breach was to occur, people in the organisation would know what to do, and the incident would more than likely be handled quicker than if there were no mitigations or plan in place.
課責原則及透過設計來達成資料保護之概念可以納入相關分析，並將其結果整合入資料控管者及資料受託運用者自身的「個人資料侵害事件處理手冊」中，以確認其營運主要階段中所涉資料運用之各方面情況。該等事前備置之手冊將能快速提供相關資訊，使資料控管者及資料受託運用者得以即時緩解風險及履行義務，而不會發生無故遲延，且能確保一旦發生個人資料侵害事故，組織成員將知道該採取哪些措施；與未事先規畫緩解措施或計畫的情況相比，能夠更快速地處理侵害事故。

14. Though the cases presented below are fictitious, they are based on typical cases from the SA's collective experience with data breach notifications. The analyses offered relate explicitly to the cases under scrutiny, but with the goal to provide assistance for data controllers in assessing their own data breaches. Any modification in the circumstances of the cases described below may result in different or more significant levels of risk, thus requiring different or additional measures. These guidelines structure the cases according to certain categories of breaches (e.g. ransomware attacks). Certain mitigating measures are called for in each case when dealing with a certain category of breaches. These measures are not necessarily repeated in each case analysis belonging to the same category of breaches. For the cases belonging to the same category only the differences are laid out. Therefore, the reader should read all cases relevant to relevant category of a breach to identify and distinguish all the correct measures to be taken.
雖然下列案例均屬虛構，但均係基於監管機關在個人資料侵害事件通報方面所累積的共同經驗所提出的典型案例。下列分析雖是針對案件具體事實

所作，但其目的係在協助資料控管者就其所涉個人資料侵害事件進行評估。下文所述案例之具體事實若有任何變更，均可能導致其風險水平有所變化或上升，從而需要採取不同或額外之措施。本指引係按個人資料侵害事件之具體類型（例如勒索軟體攻擊）來設計案例。處理不同類型的個人資料侵害事件時，可能需要採取不同的緩解措施，但這些措施也未必會在同一類型個人資料侵害事件的每個案例分析中重複分析，在屬於同一類型的不同個人資料侵害案例中，則僅會強調其中相異之處。因此，讀者應該詳閱同一類型中的所有個人資料侵害案例，以識別及區分必須採取之所有改正措施。

15. The internal documentation of a breach is an obligation independent of the risks pertaining to the breach, and must be performed in each and every case. The cases presented below try to shed some light on whether or not to notify the breach to the SA and communicate it to the data subjects affected.
就個人資料侵害事件備置內部紀錄，是獨立於個人資料侵害事件風險評估之另一項義務，且在發生任何個人資料侵害事件時均應履行。下列案例試圖說明是否應向監管機關通報個人資料侵害事件，並向受影響之當事人進行通知。

2. RANSOMWARE
勒索軟體

16. A frequent cause for a data breach notification is a ransomware attack suffered by the data controller. In these cases a malicious code encrypts the personal data, and subsequently the attacker asks the controller for a ransom in exchange for the decryption code. This kind of attack can usually be classified as a breach of availability, but often also a breach of confidentiality could occur.
通報個人資料侵害事件的常見原因是資料控管者遭受勒索軟體攻擊。於該等情況下，惡意程式碼會對個人資料進行加密，接著攻擊者就會要求控管者支付贖金以換取解密代碼。該等事件一般可被歸類為「可用性」侵害事件，但經常也可能屬「機密性」侵害事件。

2.1. CASE No. 01: Ransomware with proper backup and without exfiltration
案例 01：勒索軟體攻擊－有適當備份且未發生資料外洩的情況

Computer systems of a small manufacturing company were exposed to a ransomware attack, and data stored in those systems was encrypted. The data controller used encryption at rest, so all data accessed by the ransomware was stored in encrypted form using a state-of-the-art encryption algorithm. The decryption key was not compromised in the attack, i.e. the attacker could neither

access it nor use it indirectly. In consequence, the attacker only had access to encrypted personal data. In particular, neither the email system of the company, nor any client systems used to access it were affected. The company is using the expertise of an external cybersecurity company to investigate the incident. Logs tracing all data flows leaving the company (including outbound email) are available.

一家小型製造公司的電腦系統受到勒索軟體攻擊，並將儲存於該系統中的資料進行加密。但資料控管者採用靜態加密技術，因此所有遭勒索軟體存取的資料均係以最先進的加密演算法加密儲存；其解密金鑰在此攻擊中未遭到破解，亦即，攻擊者既無法取得金鑰，亦無法間接使用金鑰。因此，攻擊者僅能存取經過加密之個人資料。具體而言，該公司的電子郵件系統及用於存取該系統的任何客戶端系統均未受到影響。該公司委託外部網路安全公司之專家來調查此事故，並備有記載該公司所有對外資料流向（包括對外電子郵件）之日誌。

After analysing the logs and the data collected by the detection systems the company has deployed, an internal investigation supported by the external cybersecurity company determined with certainty that the perpetrator only encrypted data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to clients and employees of the company, a few dozen individuals altogether. A backup was readily available, and the data was restored a few hours after the attack took place. The breach did not result in any consequences on the day-to-day operation of the controller. There was no delay in employee payments or handling client requests.

於分析相關日誌及該公司部署之偵測系統所蒐集的資料後，由外部網路安全公司協助進行的內部調查結果確認，攻擊者僅能將資料進行加密，但無法擷取資料。相關日誌顯示，系統在遭攻擊之時段內並無資料外洩。受此事件影響的個人資料涉及數十名該公司之客戶及員工。該公司平時已有進行資料備份，因此於攻擊發生後數小時內就已完成資料還原。此事件並未對控管者之日常營運造成任何影響，向員工付款及處理客戶請求方面均未遭到任何延誤。

17. In this case, the following elements were realized from the definition of a ‘personal data breach’: a breach of security led to unlawful alteration and unauthorized access to personal data stored.

就本案例而言，我們依據「個人資料侵害事件」之定義（亦即，安全性漏

洞導致經儲存之個人資料遭非法竄改及未經授權存取）歸納出以下項目。

2.1.1. CASE No. 01 - Prior measures and risk assessment
案例 01－事前措施及風險評估

18. As with all risks posed by external actors, the likelihood that a ransomware attack is successful can be drastically reduced by tightening the security of the data controlling environment. The majority of these breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. Examples of such measures are proper patch management and the use of an appropriate anti-malware detection system. Having a proper and separate backup will help to mitigate the consequences of a successful attack should it occur. Moreover, an employee security education, training, and awareness (SETA) program, will help to prevent and recognise this kind of attack. (A list of advisable measures can be found in section 2.5.) Among those measures, a proper patch management that ensures that the systems are up to date and all known vulnerabilities of the deployed systems are fixed is one of the most important since most of the ransomware attacks exploit well known vulnerabilities.
與所有由外部行為者造成的風險相同，透過提升資料控管環境之安全性，即可大幅降低勒索軟體得逞的可能性；透過確實採取適當的組織上、物理上及技術上安全措施，即可防範多數侵害事件；該等措施包括但不限於：實施適當的漏洞修補程式及反惡意軟體偵測系統。建立適當且獨立的備份資料亦有助於緩解遭到攻擊之影響。此外，向員工提供安全訓練、教育及宣導（SETA）課程，將有助於防止及識別此等攻擊（建議採取措施之清單請參考第 2.5 段）。於該等措施中，實施適當的漏洞修補程式，確保系統處於最新狀態，且已部署系統的所有已知漏洞均已完成修復是首要任務，因為大多數勒索軟體攻擊均係利用已知安全漏洞。

19. When assessing the risks, the controller should investigate the breach and identify the type of the malicious code to understand the possible consequences of the attack. Among those risks to be considered is the risk that data was exfiltrated without leaving a trace in the logs of the systems.
在進行風險評估時，控管者應就侵害事件進行調查並識別惡意程式碼的類型，以瞭解攻擊之可能後果。需要考量的風險之一，是資料外洩並未於系統日誌中留下紀錄的情況。

20. In this example, the attacker had access to personal data and the confidentiality of cipher text containing personal data in encrypted form was compromised. However, any data that might have been exfiltrated cannot be read or used by the perpetrator, at least for the time being. The encryption technique used by the data controller conforms to the state-of-the-art. The decryption key was not

compromised and presumably could also not be determined by other means. In consequence, the confidentiality risks to the rights and freedoms of natural persons are reduced to a minimum barring cryptanalytic progress that renders the encrypted data intelligible in the future.
於本案例中，攻擊者已取得經加密之個人資料，並破壞了其中包含該等個人資料之密文（cipher text）的機密性。然而，攻擊者無法讀取或使用該等個人資料（至少目前如此）。資料控管者採用了最先進的加密技術；解密金鑰未遭破解，推測攻擊者亦無法透過其他方式識別金鑰。因此，自然人之權利及自由所面臨的機密性風險很低，除非密碼破解技術未來有所演進，使攻擊者得以讀取加密資料。

21. The data controller should consider the risk to individuals due to the breach[10]. In this case, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not compromised[11]. In this example, the adverse effects of the breach were mitigated fairly soon after the breach occurred. Having a proper backup regime[12] makes the effects of the breach less severe and here the controller was able to effectively make use of it.
資料控管者應考量當事人因本事件所面臨的風險[10]。於本案例中，當事人

---

10 For guidance on "*likely to result in high risk*" processing operations, see A29 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", WP248 rev. 01, - endorsed by EDPB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.
關於「可能導致高風險」運用作業之指導，請參考第 29 條工作小組「關於個資保護影響評估（DPIA）及基於歐盟第 2016/679 號法規之目的認定資料運用是否係屬『可能導致高風險』之指引」，第 WP248 號指引，修訂一版－經歐盟個人資料保護委員會認可，
https://ec.europa.eu/newsroom/article29/items/611236，第 9 頁。

11 Technically, encryption of data will involve "access" to original data, and in the case of ransomware, the deletion of the original – the data needs to be accessed by ransomware code to encrypt it, and to remove the original data. An attacker may take a copy of the original before deletion, but personal data will not always be extracted. As a data controller's investigation progresses, new information may come to light to make this assessment change. Access that results in unlawful destruction, loss, alteration, unauthorised disclosure of the personal data, or to a security risk to a data subject, even without interpretation of the data may be as severe as access with interpretation of the personal data.
嚴格來說，資料之加密涉及原始資料之「存取（access）」；就勒索軟體攻擊而言，資料之加密亦涉及原始資料之刪除－勒索軟體程式碼必須存取資料以對其進行加密，並刪除原始資料。攻擊者可能會在刪除原始資料前保留其副本，但不必然會從中擷取個人資料。隨著資料控制者調查的推展，新資訊可能會使評估結果有所改變。若攻擊者的存取行為導致個人資料遭非法破壞、滅失、竄改或未經授權揭露，或對當事人造成安全風險，即使攻擊者並未對個人資料進行擷取/解碼，仍可能與對個人資料造成重大影響。

12 Backup procedures should be structured, consistent and repeatable. Examples of back up procedures are the 3-2-1 method and the grandfather-father-son method. Any method should always be tested for effectiveness in coverage and when data is to be restored. Testing should also be repeated at intervals and especially when changes occur in the processing operation or its circumstances to ensure the integrity of the system.
備份作業應屬有組織、一致且可重複的程序。備份程序可採用的方式包括但不限於：「3-2-1 法」及「三代（grandfather-father-son）」法。無論採用哪種方法，均應於適用範圍內及於進行資料回復時進行測試，以確保其有效性，並應定期重複測試，特別是在資料運用作業或其相關情事發生變更時，以確保系統完整性。

之權利及自由所面臨的風險似乎起因於個人資料喪失可用性，而個人資料之機密性並未受到影響 [11]。於本案例中，侵害事件的不利影響於事件發生後很快得到緩解。平時即實施適當備份，降低了本事件的影響；本案例中，控管者亦有效地運用備份資料 [12] 來處理侵害事件。

22. On the severity of the consequences for the data subjects, only minor consequences could be identified since the affected data was restored in a few hours, the breach did not result in any consequences on the day-to-day operation of the controller and had no significant effect on the data subjects (e.g. employee payments or handling client requests).

關於當事人受此事件影響之嚴重程度，由於受影響的資料於數小時內就已完成還原，且此事件並未對控管者之日常營運造成任何影響，亦未對當事人產生重大影響（例如：向員工付款或處理客戶要求等），爰影響程度尚屬輕微。

2.1.2. CASE No. 01 – Mitigation and obligations
案例 01－緩解措施及義務

23. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again. In this particular case however, the impacts of the attack could effectively be contained by resetting all compromised systems to a clean state known to be free of malicious code, fixing the vulnerabilities and restoring the affected data soon after the attack. Without a backup, data is lost and the severity may increase because risks or impacts to individuals may also do so.
若無備份資料，控管者只能採取相當有限的措施來彌補個人資料之滅失，且相關資料均必須重新蒐集。然而，於本案例中，透過將所有遭受攻擊的系統還原至已知不含惡意程式碼的乾淨狀態、修復漏洞並於攻擊發生後很快還原受影響的資料，有效地控制此侵害事件所造成的影響。若無備份，資料就會滅失，影響的嚴重程度可能會增加，因為當事人所面臨的風險或影響也會增加。

24. The timeliness of an effective data restoration from the readily available backup is a key variable when analysing the breach. Specifying an appropriate timeframe to restore the compromised data depends on the unique circumstances of the breach at hand. The GDPR states that a personal data breach shall be notified without undue delay and, where feasible, not later than after 72 hours. Therefore, it could be determined that exceeding the 72-hour time limit is unadvisable in any case, but when dealing with high risk level cases, even complying with this deadline can be viewed as unsatisfactory.
利用備份資料有效還原資料的速度，是分析侵害事件時的關鍵變數。將遭

攻擊資料進行還原的時限，取決於該侵害事件的具體情況。GDPR 規定，知悉個人資料侵害事件後應迅即通報，不得無故遲延，且於可行之情況下，應於 72 小時內進行通報。因此可以確認，在任何情況下，通報之時間均不應晚於 72 小時；但在處理高風險事件時，僅遵守此期限仍可能被視為不太理想的處理作法。

25. In this case, following a detailed impact assessment and incident response process, the controller determined that the breach was unlikely to result in a risk to the rights and freedoms of natural persons, hence no communication to the data subjects is necessary, nor does the breach require a notification to the SA. However, as all data breaches, it should be documented in accordance with Article 33 (5). The organisation may also need (or later be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures. Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator in order to prevent any similar events in the future.
於本案例中，在經過仔細的影響評估並實施事故應變措施後，控管者確認此事件不太可能對自然人之權利及自由造成威脅，因此並無必要通知當事人，亦毋須通報監管機關。然而，與所有個人資料侵害事件相同，本事件應依據第 33 條第 5 項備置紀錄。組織可能也需要（或後續經遭監管機關要求）更新及改正其組織上及技術上之個人資料安全處理及風險緩解措施與程序。於執行更新及改正的同時，組織亦應就侵害事件進行徹底調查，並確認事發原因及攻擊者採用的方法，以防止未來發生任何類似事件。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

2.2. CASE No. 02: Ransomware without proper backup
案例 02：勒索軟體攻擊－無適當備份之情況

One of the computers used by an agricultural company was exposed to a ransomware attack and its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound

email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and clients of the company, a few dozen individuals altogether. No special categories of data were affected. No backup was available in an electronic form. Most of the data was restored from paper backups. The restoration of the data took 5 working days and led to minor delays in the delivery of orders to customers.

一家農業公司使用的其中一部電腦遭到勒索軟體攻擊，其中資料遭攻擊者加密。該公司委託外部網路安全公司之專業人員來監控其網絡，並備有記載該公司所有對外資料流向（包括對外電子郵件）之日誌。於分析相關日誌及其他偵測系統所蒐集的資料後，由外部網路安全公司協助進行的內部調查結果確認，攻擊者僅能將資料進行加密，但無法擷取資料。相關日誌顯示，系統在遭攻擊之時段內並無資料外洩。受此事件影響的個人資料涉及數十名該公司之客戶及員工。特種個料並未受到影響。該公司平日並未備置電子備份檔案。多數資料均係透過紙本備份檔案進行還原。資料還原耗費了五個工作天，導致向客戶交付訂單的時間略有延遲。

2.2.1. CASE No. 02 - Prior measures and risk assessment
案例 02－事前措施及風險評估

26. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.9. The major difference to the previous case is the lack of an electronic backup and the lack of encryption at rest. This leads to critical differences in the following steps.
資料控管者應該採取第 2.1.段及第 2.9 段(譯註：應為 2.5 段)所載之事前措施。本案例與上一個案例間的主要差異在於，本案例之控管者並未備置電子備份檔案，且未實施靜態加密，導致下列步驟亦有重大不同。

27. When assessing the risks, the controller should investigate the method of infiltration and identify the type of the malicious code to understand the possible consequences of the attack. In this example the ransomware encrypted the personal data without exfiltrating it. As a result, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not compromised. A thorough examination of the firewall logs and its implications is essential in determining

the risk. The data controller should present the factual findings of these investigations upon request.
於評估風險時，控管者應就入侵方式進行調查，並確認惡意程式碼之類型，以瞭解攻擊的潛在影響。於本案例中，勒索軟體對個人資料進行加密，但無法擷取資料。因此，當事人之權利及自由所面臨的風險似乎起因於個人資料喪失可用性，而個人資料之機密性並未受到影響。徹底檢查防火牆日誌及其關聯，對於識別風險至關重要。資料控管者應依據監管機關要求提出該等調查所發現之事實及結果。

28. The data controller needs to keep in mind that if the attack is more sophisticated the malware has the functionality to edit log files and remove the trace. So - given that logs are not forwarded or replicated to a central log server - even after a thorough investigation that determined that the personal data was not exfiltrated by the attacker, the data controller cannot state that the absence of a log entry proves the absence of exfiltration, therefore the likelihood of a confidentiality breach cannot be entirely dismissed.
資料控管者必須瞭解，若攻擊者能力強大，惡意軟體可能會有編輯日誌檔案及刪除紀錄的功能。因此－若日誌檔案並未被傳輸或複製至中央日誌伺服器－即使經過徹底調查認定個人資料並未遭攻擊者擷取，資料控管者也無法說沒有日誌就證明資料未遭外洩，因此無法完全排除此事件屬「機密性」侵害事件的可能性。

29. The data controller should assess the risks of this breach[13] if the data was accessed by the attacker. During the risk assessment, the data controller should also take into consideration the nature, the sensitivity, the volume, and the context of personal data affected in the breach. In this case no special categories of personal data are affected, and the quantity of breached data and the number of affected data subjects is low.
若資料遭攻擊者存取，資料控管者即應就該侵害事件 [13] 進行風險評估。於風險評估過程中，資料控管者亦應針對侵害事件中受影響個人資料之性質、敏感性、數量及脈絡進行考量。於本案例中，並沒有特種個資受到影響，遭攻擊資料及受影響當事人的數量均不高。

30. Gathering exact information on the unauthorized access is key for determining the risk level and preventing a new or continued attack. If the data had been copied from the database, it would obviously have been a risk-increasing factor. When uncertain about the specifics of the illegitimate access, the worse scenario should be considered and the risk should be assessed accordingly.
決定風險程度及防範新攻擊或持續攻擊的關鍵在於，針對未經授權之存取

---

13 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

事件蒐集具體資訊。若攻擊者已自資料庫中複製資料，這顯然是增加風險的因素。當無法掌握非法存取事件之具體資訊，則應考量以最壞情況來評估相關風險。

31. The absence of a backup database can be considered a risk enhancing factor depending on the severity of consequences for the data subjects resulting from the lack of availability of the data.
缺乏備份資料庫也會被認為是風險提高的因素，這取決於資料喪失可用性對當事人造成影響的嚴重性。

2.2.2. CASE No. 02 – Mitigation and obligations
案例 02－緩解措施及義務

32. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again, unless some other source is available (e.g. order confirmation e-mails). Without a backup, data may be lost and the severity will depend on the impact for the individuals.
若無備份資料，控管者只能採取相當有限的措施來彌補個人資料之滅失，且相關資料均必須重新蒐集，除非有其他資料來源（例如：確認訂單之電子郵件）。若無備份，資料可能會就此滅失，而此事件的重大程度將取決於其對當事人所造成的影響。

33. The restoration of the data should not prove to be overly problematic[14] if the data is still available on paper, but given the lack of an electronic backup database, a notification to the SA is considered necessary, as the restoration of the data took some time and could cause some delays in the orders' delivery to customers and a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.
若仍有紙本資料，還原資料應不會有太大問題[14]，但因缺乏電子備份資料，還原資料需耗費些許時間，可能會導致向客戶出貨的時程有所延遲，且相當多的後設/中繼資料（例如：日誌、時間戳記等）可能無法進行檢索，所以仍有必要通報監管機關。

34. Informing the data subjects about the breach may also depend on the length of time the personal data is unavailable and the difficulties it might cause in the operation of the controller as a result (e.g. delays in transferring employee's payments). As these delays in payments and deliveries may lead to financial loss for the individuals whose data has been compromised, one could also argue the

---

14 This will depend on the complexity and structure of the personal data. In the most complex scenarios, re-establishing data integrity, consistency with metadata, ensuring the correct relationships within data structures and checking data accuracy may take significant resources and effort.
這將取決於個人資料的複雜度及架構。在最複雜的情況下，重新建立完整資料、確保其與後設/中繼資料一致性、確保資料架構之正確關係，及檢查資料之正確性，均可能耗費大量資源與勞力。

breach is likely to result in a high risk. Also, it might not be possible to avoid informing the data subjects if their contribution is needed for restoring the encrypted data.
無法使用個人資料時間的長短，及控管者之營運是否會因此發生困難（例如：遲延支付員工工資），亦為決定是否將侵害事件通知當事人之因素。由於出貨及遲付工資都可能會導致受影響當事人之經濟損失，可能會有人認為此侵害事件恐導致高風險。此外，若需請求當事人協助還原加密資料，可能無法避免地必須通知當事人。

35. This case serves as an example for a ransomware attack with risk to the rights and freedoms of the data subjects, but not reaching high risk. It should be documented in accordance with Article 33 (5) and notified to the SA in accordance with Article 33 (1). The organisation may also need (or be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
本案例中的勒索軟體攻擊事件，對當事人的權利及自由會造成風險，但尚未達高風險的程度。此等事件應依據第 33 條第 5 項備置紀錄，並依據第 33 條第 1 項通報監管機關。組織可能也需要（或經監管機關要求）更新及改正其組織上及技術上之個人資料安全處理及風險緩解措施與程序。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	X

2.3. CASE No. 03: Ransomware with backup and without exfiltration in a hospital
案例 03：勒索軟體－發生在醫療院所、有備份且未發生資料外洩之情況

The information system of a hospital / healthcare centre was exposed to a ransomware attack and a significant proportion of its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data without exfiltrating it. The logs show no outward data flow

in the timeframe of the attack. The personal data affected by the breach relates to the employees and patients, which represented thousands of individuals. Backups were available in an electronic form. Most of the data was restored but this operation lasted 2 working days and led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering the level of service due to the unavailability of the systems.
一家醫療院所的資訊系統受到勒索軟體攻擊，其中有很大一部分資料遭攻擊者加密。該醫療院所委託外部網路安全公司之專業人員來監控其網絡，並備有記載該醫療院所所有對外資料流向（包括對外電子郵件）之日誌。於分析相關日誌及其他偵測系統所蒐集的資料後，由外部網路安全公司協助進行的內部調查結果確認，攻擊者僅能將資料進行加密，但無法擷取資料。相關日誌顯示，系統在遭攻擊之時段內並無資料外洩。受此事件影響的個人資料涉及數千名該醫療院所的員工及病患。資料係以電子形式備份。大部分資料均成功還原，但還原過程耗費兩個工作天，並因手術遭取消/延期，導致病患治療之重大延誤，且該醫療院所之服務水準亦因無法使用相關系統而下滑。

2.3.1. CASE No. 03 - Prior measures and risk assessment
案例 03－事前措施及風險評估

36. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. The major difference to the previous case is the high severity of consequences for a substantial part of the data subjects[15].
資料控管者應該採取第 2.1.段及第 2.5 段所載之事前措施。本案例與上一個案例間的主要差異在於，本案例中有大量當事人受到重大影響[15]。

37. The quantity of breached data and the number of affected data subjects are high, because hospitals usually process large quantities of data. The unavailability of the data has a high impact on a substantial part of the data subjects. Moreover, there is a residual risk of high severity to the confidentiality of the patient data.
因為醫療院所一般都會運用大量資料，所以遭攻擊之資料及受影響之當事人數量均很高。資料一旦無法使用就會對大量當事人造成重大影響。此外，病患資料之機密性也存在高度的剩餘風險。

38. The type of the breach, nature, sensitivity, and volume of personal data affected in the breach are important. Even though a backup for the data existed and it could be restored in a few days, a high risk still exists due to the severity of

[15] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

consequences for the data subjects resulting from the lack of availability of the data at the moment of the attack and the following days.
本侵害事件之類型及受侵害事件影響的個人資料之性質、敏感性及數量都很重要。即使有備份資料，且能夠在數日內還原資料，但由於遭到攻擊時及其後數日內喪失資料可用性，會使當事人受到重大影響，因此仍可能存在高風險。

2.3.2. CASE No. 03 – Mitigation and obligations
案例 03－緩解措施及義務

39. A notification to the SA is considered necessary, as special categories of personal data are involved and the restoration of the data could take a long time, resulting in major delays in patient care. Informing the data subjects about the breach is necessary due to the impact for the patients, even after restoring the encrypted data. While data relating to all patients treated in the hospital during the last years have been encrypted, only those patients who were scheduled to be treated in the hospital during the time the computer system was unavailable were impacted. The controller should communicate the data breach to those patients directly. Direct communication to the other patients some of which may not have been in the hospital for more than twenty years may not be required due to the exception in Article 34 (3) c). In such a case, there shall instead be a public communication[16] or similar measure whereby the data subjects are informed in an equally effective manner. In this case, the hospital should make the ransomware attack and its effects public.
此事件必須通報監管機關，因為涉及特種個資，且還原資料可能需要很長時間，因而導致病患照護發生重大延誤。由於事件會使病患受到影響，即使在還原加密資料後，仍有必要告知當事人。雖然過去幾年曾於該醫療院所接受治療的所有病患相關資料均遭攻擊者加密，但只有在電腦系統無法使用期間原訂接受治療的病患有受到影響。控管者應該直接向該等病患通知個人資料侵害事件之情況。由於第 34 條第 3 項第 c 款所載例外情事，若病患已超過 20 年未造訪該醫療院所，可能就毋須直接向其發送通知；於此情況下，則應透過公告 [16] 或類似方式，使當事人得以同樣有效的方式知悉個人資料侵害事件。於本案例中，該醫療院所應將勒索軟體攻擊事件及其

---

16 GDPR Recital 86 explains that "*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*".
GDPR 前言第 86 段說明：「*應於合理可行之情況下盡快通知當事人，並與監管機關密切合作，遵循監管機關或其他相關單位（如執法機關）提供之指導。例如，若有發生損害之立即風險需要緩解時，就需要迅即通知當事人，而若需要實施適當措施來防止持續或類似之個資侵害事件，則較有理由在較長時間後始為通知*」。

影響公布於眾。

40. This case serves as an example for a ransomware attack with high risk to the rights and freedoms of the data subjects. It should be documented in accordance with Article 33 (5), notified to the SA in accordance with Article 33 (1) and communicated to the data subjects in accordance with Article 34 (1). The organisation also needs to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
本案可作為對當事人之權利及自由具有高風險之勒索軟體攻擊之例子。應依據第 33 條第 5 項對其進行紀錄，依據第 33 條第 1 項通報監管機關，並依據第 34 條第 1 項通知當事人。該組織亦須要更新及改正其組織上及技術上之個人資料安全處理及風險緩解措施及程序。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

2.4. CASE No. 04: Ransomware without backup and with exfiltration
案例 04：勒索軟體攻擊－無備份且有發生資料外洩之情況

The server of a public transportation company was exposed to a ransomware attack and its data was encrypted by the attacker. According to the findings of the internal investigation the perpetrator not only encrypted the data, but also exfiltrated it. The type of breached data was the personal data of clients and employees, and of the several thousand people using the services of the company (e.g. buying tickets online). Beyond basic identity data, identity card numbers and financial data such as credit card details are involved in the breach. A backup database existed, but it was also encrypted by the attacker.
一家大眾運輸公司的伺服器遭到勒索軟體攻擊，資料遭攻擊者加密。內部調查結果發現，攻擊者不僅加密資料且成功擷取資料。遭侵害資料之類型，為客戶、員工及數千名該公司服務（例如線上購票服務）使用者之個人資料。除了基本的身分資料外，此侵害事件亦涉及身分證字號及財務資料（例如信用卡詳細資訊）。該公司設有備份資料庫，但也遭攻擊者加密。

2.4.1. CASE No. 04 - Prior measures and risk assessment
案例 04－事前措施及風險評估

41. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. Though backup was in place, it was also affected by the attack. This arrangement alone raises questions about the quality of the controller's prior IT security measures and should be further scrutinised during the investigation, since in a well-designed backup regime, multiple backups must be securely stored without access from the main system, otherwise they could be compromised in the same attack. Furthermore, ransomware attacks may lie undiscovered for days slowly encrypting rarely used data. This can render multiple backups useless, so backups should also be taken periodically and be isolated. This would increase the likelihood of recovery albeit with increased loss data.
資料控管者應該採取第 2.1.段及第 2.5 段所載之事前措施。雖然有備份資料，但備份資料也受到侵害事件之影響。這顯示出控管者的事前資安措施品質有問題，且應於調查期間接受進一步檢視；因為在設計完善的備份機制下，應會以安全的方式儲存多份備份資料，且該等備份資料應無法從主系統存取，否則也同樣會在侵害事件中受到損害。此外，勒索軟體攻擊可能會在已經發生數日後才被發現，勒索軟體會慢慢地加密很少使用的資料；這可能會讓多份備份資料無法發揮作用，所以備份作業亦應定期辦理且每份備份資料應分開儲存。透過前述措施，即使有較大量資料滅失，惟還原資料的機會仍然很高。

42. This breach concerns not only data availability, but confidentiality as well, since the attacker may have modified and / or copied data from the server. Therefore, the type of the breach results in high risk[17].
此侵害事件不僅涉及到資料可用性，亦涉及到機密性，因為攻擊者可能已變更及/或複製伺服器上之資料。因此，此類型侵害事件會導致高風險[17]。

43. The nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data. Beyond basic identity data, identity documents and financial data such as credit card details are involved too. A data breach concerning these types of data presents high risk in and of themselves, and if processed together, they could be used for – among others - identity theft or fraud.
個人資料之性質、敏感性及數量均為進一步提高風險的因素，因為受影響的人數眾多，受影響的個人資料整體數量也會很高。除基本身分資料外，也涉及身分文件及財務資料（如信用卡詳細資訊）。涉及該等類型資料之個人資料侵害事件本身就存在很高的風險，該等類型之資料若同時遭外洩，即可能被用於（包括但不限於）身分冒用或詐欺。

---

17 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

44. Due to either faulty server logic or organizational controls, the backup files were affected by the ransomware, preventing the restore of data and enhancing the risk.
由於伺服器之邏輯或組織控管發生錯誤，備份檔案因此受到勒索軟體影響而無法還原資料，風險因而提升。

45. This data breach presents a high risk to the rights and freedoms of individuals, because it could likely lead to both material (e.g. financial loss since credit card details were affected) and non-material damage (e.g. identity theft or fraud since identity card details were affected).
此個人資料侵害事件對當事人之權利及自由構成高風險，因為可能會導致財物（例如：因信用卡詳細資訊受影響而造成的財務損失）及非財物損害（例如：因身分證資訊受影響而造成之身分冒用或詐欺）。

2.4.2. CASE No. 04 – Mitigation and obligations
案例 04－緩解措施及義務

46. Communication to the data subjects is essential, so they can make the necessary steps to avoid material damage (e.g. block their credit cards).
必須通知當事人，使當事人得以採取必要措施來避免財物損失（例如，通知銀行止付信用卡）。

47. Aside from documenting the breach in accordance with Article 33 (5), a notification to the SA is also mandatory in this case (Article 33 (1)) and the controller is also obliged to communicate the breach to the data subjects (Article 34 (1)). The latter could be undertaken on a person-by-person basis, but for individuals where contact data is not available the controller should do so publicly, provided that such communication would not be susceptible to trigger additional negative consequences on the data subjects, e.g. by way of a notification on its website. In the latter case a precise and clear communication is required, in plain sight on the homepage of the controller, with exact references of the relevant GDPR provisions. The organisation may also need to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
除依據第 33 條第 5 項記錄個人資料侵害事件外，於本案例中，控管者必須將個人資料侵害事件通報監管機關（第 33 條第 1 項），亦有義務通知當事人（第 34 條第 1 項）；後者得對個人逐一通知，但若無當事人之聯絡資訊，控管者應透過公開方式進行通知（例如於其網站上張貼公告），但前提為不得對當事人造成額外之不利影響。以公開方式為通知時，必須於控管者網站首頁上發布精確及清晰之公告，並正確引用相關的 GDPR 條款。該組織可能亦須更新及改正其組織上及技術上之個人資料安全處理及風險緩解措施及程序。

Actions necessary based on the identified risks 依據經識別風險所必須採取的行動		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

2.5. Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks
防範勒索軟體攻擊/緩解其影響之組織上及技術上措施

48. The fact that a ransomware attack could have taken place is usually a sign of one or more vulnerabilities in the controller's system. This also applies in ransomware cases in which the personal data has been encrypted, but has not been exfiltrated. Regardless of the outcome and the consequences of the attack, the importance of an all-encompassing evaluation of the data security system - with particular emphasis on IT security cannot be stressed enough. The identified weaknesses and security holes are to be documented and addressed without delay.
可能發生勒索軟體攻擊之事實，通常顯示出控管者的系統存在一項或多項漏洞。這也適用個人資料遭到加密但未遭外洩的勒索軟體攻擊事件。無論攻擊事件之結果及後果如何，均絕對必須針對資料安全系統進行全面評估一且應特別著眼於資訊科技安全。評估結果所發現的安全性弱點及漏洞應進行記錄並立即改正。

49. Advisable measures:
建議之措施：

(The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.)
（下列措施並非詳盡完整清單。列舉下列措施之用意在於提供防範構思及可能的解決方案。因資料運用活動性質不同，控管者應自行決定最適合特定情況的措施。）

- Keeping the firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) up to date. Ensuring that appropriate IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. This includes keeping detailed logs of which patches are applied at which timestamp.

確保伺服器、客戶端設備、活動網絡元件及設置於同一局部區域網絡（LAN）上的任何其他裝置（包括無線網路設備）上的韌體、作業系統及應用程式軟體均已更新至最新版本。實施適當的資訊科技安全措施，確保該等措施之有效性，並於資料運用或相關情事發生變化或演變時，確保其定期更新至最新版本，包括備置並維持詳細日誌，以記錄實施漏洞修補的確切時間點（其時間戳記）。

- Designing and organising processing systems and infrastructure to segment or isolate data systems and networks to avoid propagation of malware within the organisation and to external systems.
設計及規劃資料運用系統及基礎設施，以分割或隔離資料系統及網絡，避免惡意軟體於組織內部及外部系統之傳播。

- The existence of an up-to-date, secure and tested backup procedure. Media for medium- and long-term back-up should be kept separate from operational data storage and out of reach of third parties even in case of a successful attack (such as daily incremental backup and weekly full backup).
採用最新、安全且經測試之備份程序。用於中長期備份之媒體應與營運資料儲存設備分開，即使發生攻擊事件，也不能讓第三方接觸該等備份（例如：每日備份及每週備份）。

- Having / obtaining an appropriate, up-to-date, effective and integrated anti-malware software.
部署/取得適當、最新、有效及整合型之反惡意軟體。

- Having an appropriate, up-to-date, effective and integrated firewall and intrusion detection and prevention system. Directing network traffic through the firewall/intrusion detection, even in the case of home office or mobile work (e.g. by using VPN connections to organizational security mechanisms when accessing the internet).
部署適當、最新、有效及整合型之防火牆及入侵偵測及預防系統。透過防火牆/入侵偵測引導網絡流量，即使是在居家辦公或行動辦公的情況下亦然（例如，於連接網絡時採用虛擬私人網絡（VPN）連接至組織安全機制）。

- Training employees on the methods of recognising and preventing IT attacks. The controller should provide means to establish whether emails and messages obtained by other means of communication are authentic and trustworthy. Employees should be trained to recognize when such an attack has realized, how to take the endpoint out of the network and their obligation to immediately report it to the security officer.
針對識別及預防資訊科技攻擊之方法辦理員工教育訓練。控管者應提供方法，協助員工辨別電子郵件及透過其他通訊方式取得的資訊是否為真

實可信。員工應該接受教育訓練，以瞭解該等事件之攻擊模式，如何將相關端點自網絡中移除，及其有義務立即通報資安主管。

- Emphasize the need of identifying the type of the malicious code to see the consequences of the attack and be able to find the right measures to mitigate the risk. In case a ransomware attack has succeeded and there is no back-up available, tools available such as the ones by the "no more ransom" (nomoreransom.org) project may be applied to retrieve data. However, in case a safe backup is available, restoring the data from it is advisable.
  務必識別惡意程式碼之類型，以瞭解攻擊事件之後果，並找出正確措施來緩解風險。若系統確實遭勒索軟體入侵且沒有備份資料，則可以運用「反勒贖（No More Ransom）」平台（nomoreransom.org）所提供之工具等來取回資料。然而，若有安全備份資料，則建議以備份來還原資料。
- Forwarding or replication all logs to a central log server (possibly including the signing or cryptographic time-stamping of log entries).
  將所有日誌轉發或複製到中央日誌伺服器（亦得包括對日誌條目簽名或加密時間戳記）。
- Strong encryption and multi factor authentication, in particular for administrative access to IT systems, appropriate key and password management.
  採用嚴密的加密及多因素驗證技術，特別是資訊科技系統之管理存取權限、適當的金鑰及密碼管理。
- Vulnerability and penetration testing on a regular basis.
  定期進行漏洞及滲透測試。
- Establish a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) within the organization, or join a collective CSIRT/CERT. Create an Incident Response Plan, Disaster Recovery Plan and a Business Continuity Plan, and make sure that these are thoroughly tested.
  於組織內部建立電腦安全事故應變小組（CSIRT）或電腦緊急應變小組（CERT），或加入 CSIRT/CERT 組織。訂定事故應變計畫、災難復原計畫及業務連續性計畫，並確保該等計畫皆經徹底測試。
- When assessing countermeasures – risk analysis should be reviewed, tested and updated.
  於評估應變措施時，應檢視、測試及更新風險分析。

3. DATA EXFILTRATION ATTACKS
資料外洩攻擊

50. Attacks that exploit vulnerabilities in services offered by the controller to third parties over the internet, e.g. committed by way of injection attacks (e.g. SQL

injection, path traversal), website compromising and similar methods, may resemble ransomware attacks in that the risk emanates from the action of an unauthorized third party, but those attacks typically aim at copying, exfiltrating and abusing personal data for some malicious end. Hence, they are mainly breaches of confidentiality and, possibly, also data integrity. At the same time, if the controller is aware of the characteristics of this kind of breaches, there are many measures available to controllers that can substantially reduce the risk of a successful execution of an attack.

有些攻擊者會利用控管者在網路上向第三方提供服務中之漏洞（例如透過注入攻擊（如 SQL 注入（SQL Injection）、路徑遍歷（path traversal）等）或網站入侵及類似方法進行攻擊，此等攻擊可能與勒索軟體攻擊類似，因為風險來自於未經授權第三方之行動，但一般係為複製、擷取及濫用個人資料以達到特定惡意目的。因此，此等攻擊主要屬於「機密性」侵害事件，但亦可能屬「完整性」侵害事件。另外，若控管者瞭解此等個人資料侵害事件之特點，即可採取多項措施來大幅降低遭攻擊的風險。

3.1. CASE No. 05: Exfiltration of job application data from a website
案例 05：網站之求職資料外洩

An employment agency was the victim of a cyber-attack, which placed a malicious code on its website. This malicious code made personal information submitted through online job application forms and stored on the webserver accessible to unauthorized person(s). 213 such forms are possibly affected, after analysing the affected data it was determined that no special categories of data were affected in the breach. The particular malware toolkit installed had functionalities that allowed the attacker to remove any history of exfiltration and also allowed processing on the server to be monitored and to have personal data captured. The toolkit was discovered only a month after its installation.

一家就業仲介機構遭到網路攻擊，攻擊者於其網站上放置惡意程式碼，未經授權存取透過線上求職表單提交並儲存於網路伺服器上的個人資料。可能有 213 份該等表單受到影響；在分析受影響資料後，判斷認為並無特種個資於本次攻擊中受到影響。該網站遭放置的惡意軟體中，有工具箱可允許攻擊者刪除任何資料擷取紀錄，還能監控並擷取在伺服器上運用之個人資料。該工具箱放置後一個月才被發現。

3.1.1. CASE No. 05 - Prior measures and risk assessment
案例 05－事前措施及風險評估

51. The security of the data controller's environment is extremely important, as the

majority of these breaches can be prevented by ensuring that all systems are constantly updated, sensitive data is encrypted and applications are developed according to high security standards like strong authentication, measures against brute force, attacks, "escaping" or "sanitising"[18] user inputs, etc. Periodic IT security audits, vulnerability assessments and penetration tests are also required in order to detect these kinds of vulnerabilities in advance and fix them. In this particular case, file integrity monitoring tools in production environment might have helped to detect the code injection. (A list of advisable measures is to be found in section 3.7).

資料控管者之環境安全非常重要，因為大多數此類型漏洞均可透過持續更新系統、加密敏感性資料，及採用高資安標準（例如：高強度驗證機制、防止暴力攻擊之措施、「轉義（escaping）」或「淨化（sanitising）」[18]使用者輸入資訊等）進行應用程式開發來有效防範；另外亦須定期進行資訊科技安全稽核、漏洞評估及滲透測試，俾以提前發現該等類型之漏洞並加以修復。於本案例中，生產環境中的文件完整性監控工具可能有助於偵測攻擊程式碼之入侵（建議措施清單請參考第 3.7 段）。

52. The controller should always start to investigate the breach by identifying the type of the attack and its methods, in order to assess what measures are to be taken. To make it fast and efficient, the data controller should have an incident response plan in place which specifies the swift and necessary steps to take control over the incident. In this particular case, the type of the breach was a risk enhancing factor since not only was data confidentiality curtailed, the infiltrator also had the means to establish changes in the system, so data integrity also became questionable.

控管者應持續透過識別攻擊類型及方法來展開個人資料侵害事件之調查，以評估該採取哪些措施。為確保調查快速、有效，資料控管者應備置事故應變計畫，於其中載明應立即採取之必要措施，以控管事故後續。於本案例中，侵害事件之類型為提高風險的因素之一，因為攻擊者不僅會破壞資料之機密性，亦會就系統進行變更，所以資料之完整性也會受到影響。

53. The nature, sensitivity and volume of personal data affected in the breach should be assessed to determine to what extent the breach affected the data subjects. Though no special categories of personal data were affected, the accessed data contains considerable information about the individuals from the online forms, and such data could be misused in a number of ways (targeting with unsolicited marketing, identity theft, etc.), so the severity of the consequences should increase

---

[18] Escaping or sanitizing user inputs is a form of input validation, which ensures that only properly formatted data is entered into an information system.
轉義（escaping）或淨化（sanitizing）使用者輸入資訊，為一種輸入驗證形式，確保只有格式正確的資料才能輸入至資訊系統中。

the risk to the rights and freedoms of the data subjects[19].
應評估侵害事件中受影響個人資料之性質、敏感性及數量，以判斷侵害事件對當事人之影響程度。雖然沒有特種個資受到影響，但被存取之資料包含來自線上表單之大量個人資料，該等資料可能被以多種方式濫用（針對特定對象進行未經請求的行銷、身分冒用等），該等重大影響會提高對當事人權利及自由之風險[19]。

3.1.2. CASE No. 05 – Mitigation and obligations
案例 05－緩解措施及義務

54. If possible, after solving the problem, the database should be compared with the one stored in a secure backup. The experiences drawn from the breach should be utilized in updating the IT infrastructure. The data controller should return all affected IT systems to a known clean state, remedy the vulnerability and implement new security measures to avoid similar data breaches in the future, e.g. file integrity checks and security audits. If personal data was not only exfiltrated, but also deleted, the controller has to take systematic action to recover the personal data in the state it was in before the breach. It may be necessary to apply full backups, incremental changes and then possibly rerun the processing since the last incremental backup – which requires that the controller is able to replicate the changes made since the last backup. This could require that the controller has the system designed to retain the daily input files in case they need to be processed again and requires a robust method of storage and a suitable retention policy.
若可能，在解決問題後，應將資料庫與儲存於安全備份中的資料庫進行比較，並應利用自侵害事件中得出的經驗，更新資訊科技基礎設施。資料控管者應將所有受影響之資訊科技系統還原到已知之原始/清潔狀態、改正漏洞並實施新的安全措施（例如文件完整性檢查及安全稽核），以避免未來發生類似的個人資料侵害事件。若個人資料不僅遭外洩且遭刪除，控管者必須採取全面之系統性行動，將個人資料還原到資料外洩前的狀態。控管者可能必須運用完整備份，實施逐步變更，並可能從最後一次進行備份的時間點起重新進行資料運用－但前提是控管者必須能夠複製最後一次備份以來之變更。控管者因此可能需要透過系統設計來保留每日之輸入文件，以防需要再次進行資料運用，並須採取穩健的儲存方法及適當的保存政策。

55. In light of the above, as the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects should definitely be informed about it (Article 34(1)), which of course means that the relevant SA(s) should also be involved in the form of a data breach notification. Documenting the breach is obligatory according to Article 33 (5) GDPR and makes the assessment of the

---

19 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

situation easier.
基於上述，因個人資料侵害事件可能使自然人之權利及自由面臨高風險，控管者必須將個人資料侵害事件通知當事人（第 34 條第 1 項），亦必須通報相關監管機關。GDPR 第 33 條第 5 項強制規定應就個人資料侵害事件備置記錄，這將使事件評估較容易進行。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

3.2. CASE No. 06: Exfiltration of hashed password from a website
案例 06：網站之雜湊密碼外洩

An SQL Injection vulnerability was exploited to gain access to a database of the server of a cooking website. Users were only allowed to choose arbitrary pseudonyms as usernames. The use of email addresses for this purpose was discouraged. Passwords stored in the database were hashed with a strong algorithm and the salt was not compromised. Affected data: hashed passwords of 1.200 users. For safety's sake, the controller informed the data subjects about the breach via e-mail and asked them to change their passwords, especially if the same password was used for other services.
駭客利用 SQL 注入（SQL Injection）安全性漏洞非法存取一烹飪網站之伺服器資料庫。此網站要求使用者僅得選用隨機假名作為帳號名稱，並請使用者避免將其電子郵件地址用於使用者帳密中。該資料庫所保存的使用者密碼係透過安全性強的演算法進行雜湊，其鹽值並未遭到破解。受影響之資料：1,200 名使用者的雜湊密碼。為安全起見，控管者透過電子郵件通知該等當事人，並請他們變更密碼，特別是如果同一組密碼也有用在其他地方。

3.2.1. CASE No. 06 - Prior measures and risk assessment
案例 06－事前措施及風險評估

56. In this particular case data confidentiality is compromised, but the passwords in the database were hashed with an up-to-date method, which would decrease the

risk regarding the nature, sensitivity, and volume of personal data. This case presents no risks to the rights and freedoms of the data subjects.
於本案例中，個人資料機密性已受到損害，但因資料庫中的密碼係透過最新技術進行雜湊，個人資料相關風險在性質、敏感程度及數量方面均有所緩解。於本案例中，當事人之權利及自由並未遭受任何風險。

57. Furthermore, no contact information (e.g. e-mail addresses or phone numbers) of data subjects was compromised, which means there is no significant risk for the data subjects of being targeted by fraud attempts (e.g. receiving phishing e-mails or fraudulent text messages and phone calls). No special categories of personal data were involved.
此外，當事人的聯絡資訊（例如電子郵件地址、電話號碼等）並未遭竊，這表示當事人不會面臨成為詐騙對象（例如收到網路釣魚（phishing）電子郵件或詐騙簡訊及電話等）的顯著風險。本案例並未涉及特種個人資料。

58. Some user names could be regarded as personal data, but the subject of the website does not allow for negative connotations. Although it has to be noted that the risk assessment may change[20], if the type of the website and the data accessed could reveal special categories of personal data (e. g. website of a political party or trade union). Using state of the art encryption could mitigate the adverse effects of the breach. Assuring that a limited number of attempts to login is allowed will prevent brute force login attacks to be successful, thus reducing largely the risks imposed by attackers already knowing the usernames.
有些帳號名稱得被視為個人資料，惟此網站並不允許使用者採用具有負面含意之帳號名稱。惟需注意者為，若網站類型及被存取的資料可能含有特種個人資料（例如涉及政黨或工會網站之情況），則上述風險評估即可能有所不同[20]。採用最新加密技術可以緩解個人資料侵害事件帶來的不利影響。確實限制嘗試登入次數可防範使用者密碼遭暴力破解，從而大幅降低已掌握使用者帳號之駭客所帶來的風險。

3.2.2. CASE No. 06 – Mitigation and obligations
案例 06－緩解措施及義務

59. The communication to the data subjects in some cases could be considered a mitigating factor, since the data subjects are also in a position to make the necessary steps to avoid further damages from the breach, for example by changing their password. In this case, notification was not mandatory, but in many cases it can be considered a good practice.
在特定情況下，向當事人發送通知得被視為緩解措施，因當事人接獲通知

---

20 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

後將得以採取必要措施（例如變更密碼等）以避免因該個人資料侵害事件遭受進一步損害。於本案例中，控管者並不具通知義務，但在許多情況下，發送通知會被視為適當作法。

60. The data controller should correct the vulnerability and implement new security measures to avoid similar data breaches in the future like, for example, systematic security audits to the website.
資料控管者應修補安全性漏洞並實施新的安全維護措施，以避免未來再度發生類似之個人資料侵害事件，例如對網站進行系統性之資安稽核。

61. The breach should be documented in accordance with Article 33 (5) but no notification or communication needed.
個人資料侵害事件應依據第 33 條第 5 項備置紀錄，但無須為通報或通知。

62. Also, it is strongly advisable to communicate a breach involving passwords to data subjects in any case even when the passwords were stored using a salted hash with an algorithm conforming to the state-of-the-art. The use of authentication methods obviating the need to process passwords on the server side is preferable. Data subjects should be given the choice to take appropriate measures regarding their own passwords.
此外，強烈建議無論如何均應將涉及使用者密碼的個人資料侵害事件通知當事人，即使該等密碼之保存係採用符合最新技術之演算法進行加鹽雜湊亦然。驗證方法應採用毋須於伺服器端處理密碼者為宜。應讓當事人自行選擇對其密碼採取適當措施。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

3.3. CASE No. 07: Credential stuffing attack on a banking website
案例 07：銀行網站遭憑證填充攻擊

A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were

leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.

一家銀行的網路銀行遭到網路攻擊。攻擊者利用一組固定瑣碎密碼列出所有可能的使用者帳號組合。該等密碼由 8 位數字組成。由於網站漏洞，於特定情況下，當事人之資訊（姓名、性別、出生日期及地點、財務代碼、使用者識別碼）會洩露給攻擊者，即使攻擊者輸入的密碼不正確或銀行帳戶已經閒置不用亦然。此攻擊事件影響約 10 萬名當事人。其中，攻擊者成功登入約 2,000 個帳戶，該等帳戶使用的是攻擊者嘗試的瑣碎密碼。控管者於事後得以識別所有非法登入嘗試，並透過反詐欺檢查確認該等帳戶於攻擊期間沒有進行任何交易。銀行之所以會發現該個人資料侵害，是因為其資安作業中心偵測到大量針對該網站之登入請求。控管者的應變措施是關閉網站來阻止任何人登入網站，並強制重設遭攻擊帳戶之密碼。控管者僅向持有遭入侵帳戶之使用者（即密碼遭破解或資料遭揭露的使用者）通知該個人資料侵害事件。

3.3.1. CASE No. 07 - Prior measures and risk assessment
案例 07－事前措施及風險評估

63. It is important to mention that controllers handling data of highly personal nature[21] have a larger responsibility in terms of providing adequate data security, e.g. having a security operation's centre and other incident prevention, detection and response measures. Not meeting these higher standards will certainly result in

[21] Such as information of the data subjects referred to payment methods such as card numbers, bank accounts, online payment, payrolls, bank statements, economic studies or any other information that may reveal economic information pertaining to the data subjects.
例如：當事人之資訊中含有支付方式，如卡號、銀行帳戶、線上支付、薪資單、銀行帳單、經濟研究或任何其他可能揭露與當事人相關之經濟資訊。

more serious measures during an SA's investigation.
首需強調者為，若控管者所處理的個人資料屬高度重要性質[21]，在確保資料安全方面就負有較大責任，例如，設立資安作業中心及其他事故預防、偵測及應變措施。若無法達成該等高標準，在面臨監管機關調查時將會被要求採取更嚴格的措施。

64. The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high.
此個人資料侵害事件涉及身分及使用者帳號資訊以外之金融資料，因此影響特別重大。受影響人數眾多。

65. The fact that a breach could happen in such a sensitive environment points to significant data security holes in the controller's system, and may be an indicator of a time when the review and update of affected measures is "necessary" in line with Articles 24 (1), 25 (1), and 32 (1) of the GDPR. The breached data permits the unique identification of data subjects and contains other information about them (including gender, date and place of birth), furthermore it can be used by the attacker to guess the customers' passwords or to run a spear phishing campaign directed at the bank customers.
在此敏感環境中會發生個人資料侵害事件，顯示出控管者的系統存在重大的資料安全性漏洞，且必須依據 GDPR 第 24 條第 1 項、第 25 條第 1 項及第 32 條第 1 項，檢視及更新受影響之措施。洩漏的資料使攻擊者可單獨識別當事人身分，且其中包含當事人之其他資訊（包括性別、出生日期及地點）；此外，攻擊者亦可利用該等資料來猜測銀行客戶密碼或針對銀行客戶進行魚叉式網路釣魚（spear phishing）詐騙。

66. For these reasons, the data breach was deemed likely to result in a high risk to the rights and freedoms of all the data subjects concerned[22]. Therefore, the occurrence of material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud) is a conceivable outcome.
基於上述原因，此個人資料侵害事件被認為會使所有相關當事人之權利及自由面臨高風險[22]，因此可能發生財物（如財務損失）及非財物損害（如身分冒用或詐欺）。

3.3.2. CASE No. 07 – Mitigation and obligations
案例 07－緩解措施及義務

67. The controller's measures mentioned in the case description are adequate. In the wake of the breach it also corrected the vulnerability of the website and took other steps to prevent similar future data breaches, such as adding two-factor

---

22 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

authentication to the concerned website and moving up to a strong customer authentication.
於本案例中，控管者所採取之措施應屬充分。於個人資料侵害事件發生後，控管者改正網站漏洞並採取其他措施來防止未來發生類似的個人資料侵害事件，如於相關網站上加入雙因素驗證機制，並採用較嚴格的客戶驗證程序。

68. Documenting the breach according to Article 33 (5) GDPR and notifying the SA about it are not optional in this scenario. Furthermore, the controller should notify all 100.000 data subjects (including the data subjects whose accounts were not compromised) in accordance with Article 34 GDPR.
於本案例中，控管者必須依據 GDPR 第 33 條第 5 項記錄個人資料侵害事件並通報監管機關。此外，控管者亦應依據 GDPR 第 34 條通知所有（10 萬名）當事人（包括帳戶未受影響的當事人）。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

3.4. Organizational and technical measures for preventing / mitigating the impacts of hacker attacks
防範駭客攻擊/緩解其影響之組織上及技術上措施

69. Just as in case of ransomware attacks, regardless of the outcome and the consequences of the attack, reevaluating IT security is compulsory for controllers in similar cases.
如同勒索軟體攻擊事件，無論攻擊事件結果及後果如何，面臨類似情況的控管者均必須重新評估其資訊科技安全措施。

70. Advisable measures[23]:
建議之措施[23]：

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on*

[23] For secure web application development see also: https://www.owasp.org/index.php/Main_Page.
關於安全的網路應用程式開發，另參考：https://www.owasp.org/index.php/Main_Page。

which measures fit the given situation the most.)
（下列措施並非詳盡完整清單。列舉下列措施之用意在於提供防範構思及可能的解決方案。因資料運用活動性質不同，控管者應自行決定最適合特定情況的措施。）

- State-of-the-art encryption and key management, especially when passwords, sensitive or financial data are being processed. Cryptographic hashing and salting for secret information (passwords) is always preferred over encryption of passwords. The use of authentication methods obviating the need to process passwords on the server side is preferable.
  採用最先進的加密及金鑰管理機制，特別是在處理密碼、敏感性或金融資料時。秘密資訊（密碼）之加密雜湊（cryptographic hashing）及加鹽（salting）優於密碼加密。最好採用驗證機制，以避免需於伺服器端處理密碼。

- Keeping the system up to date (software and firmware). Ensuring that all IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. In order to be able to demonstrate compliance with Article 5(1)(f) in accordance with Article 5 (2) GDPR the controller should maintain a record of all updates performed, including also the time when they were applied.
  確保系統更新至最新版本（軟體及韌體）。實施所有資訊科技安全措施，確保該等措施之有效性，並於資料運用或相關情事發生變化或演變時，確保其定期更新至最新版本。為能夠依據 GDPR 第 5 條第 2 項證明其遵守第 5 條第 1 項第 f 款規定，控管者應備置並維持所有更新紀錄，其中應包括安裝該等更新的時間。

- Use of strong authentication methods like two-factor authentication and authentication servers, complemented by an up-to-date password policy.
  採用嚴格的驗證機制，如雙因素驗證及驗證伺服器，並搭配最新的密碼政策。

- Secure development standards include the filtering of user input (using white listing as far as practicable), escaping user inputs and brute force prevention measures (such as limiting the maximum amount of retries). “Web Application Firewalls” may assist in the effective use of this technique.
  安全開發標準包括過濾使用者輸入資訊（盡可能採用白名單機制）、轉義（escaping）使用者輸入資訊及預防暴力破解措施（如限制重試次數上線）。「網路應用防火牆」可協助有效部署該等技術。

- Strong user privileges and access control management policy in place.
  制訂嚴格的使用者權限及存取權限控管政策。

- Use of appropriate, up-to-date, effective and integrated firewall, intrusion

detection and other perimeter defence systems.
採用適當、最新、有效且整合型防火牆、入侵偵測及其他周邊防禦系統。

- Systematic IT security audits and vulnerability assessments (penetration testing).
執行有系統的資訊科技安全稽核及漏洞評估（滲透測試）。
- Regular reviews and testing to ensure that backups can be used to restore any data whose integrity or availability was affected.
實施定期檢視及測試，以確保備份可用於還原其完整性或可用性受到影響之任何資料。
- No session ID in URL in plain text.
在純文字網址中不使用對談識別碼（session ID）。

4. INTERNAL HUMAN RISK SOURCE
內部人為風險來源

71. The role of human error in personal data breaches has to be highlighted, due to its common appearance. Since these types of breaches can be both intentional and unintentional, it is very hard for the data controllers to identify the vulnerabilities and adopt measures to avoid them. The International Conference of Data Protection and Privacy Commissioners recognized the importance of addressing such human factors and adopted the resolution to address the role of human error in personal data breaches in October 2019[24]. This resolution stresses that appropriate safeguarding measures should be taken to prevent human errors and provides a non-exhaustive list of such safeguards and approaches.
個人資料侵害事件中必須特別注意人為錯誤所扮演的角色，因為人為錯誤很常見。由於該等類型之個人資料侵害事件有可能是蓄意也可能是無心造成，資料控管者很難識別漏洞並採取措施避免該等漏洞。資料保護及隱私權專員國際會議（International Conference of Data Protection and Privacy Commissioners）瞭解解決該等人為因素的重要性，並於 2019 年 10 月針對人為錯誤於個人資料侵害事件中所扮演角色作成決議[24]。該決議強調應採取適當防禦措施來防範人為錯誤，並提供該等防禦措施及方法之示例清單。

4.1. CASE No. 08: Exfiltration of business data by an employee
案例 08：員工洩漏業務資料

During his period of notice, the employee of a company copies business data from the company's database. The employee is authorized to access the data

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

only to fulfill his job tasks. Months later, after quitting the job, he uses the data thus gained (basic contact data) to feed a new data processing for which he is the controller in order to contact the clients of the company to entice them to his new business.
一家公司之員工於離職預告期間自公司資料庫中複製業務資料。該員工被授權僅得為履行其職務而存取該等資料。該員工辭職幾個月後，使用他藉此取得的資料（基本聯絡資訊）為新的資料運用（其為控管者），即聯絡該公司客戶，為其新公司之業務招攬。

4.1.1. CASE No. 08 - Prior measures and risk assessment
案例 08－事前措施及風險評估

72. In this particular case no prior measures were taken to prevent the employee from copying contact information of the company's clientele, since he needed – and had – legitimate access to this information for his job tasks. Since fulfilling most customer relation jobs require some kind of employee access to personal data, these data breaches may be the most difficult to prevent. Limitations to the scope of access may limit the work the given employee is able to do. However, well thought out access policies and constant control can help prevent such breaches.
於本案例中，公司並未採取措施防止該員工複製公司客戶之聯絡資訊，因為該員工需要－且確實有－合法存取該等資訊來履行其職務。因為在執行大多數客戶關係工作時，員工均需要存取特定個人資料，該等個人資料侵害事件可能是最難預防的類型。針對存取範圍進行限制可能會使員工履行職務受到限制。然而，完善的存取權限政策及持續的控管，可以協助防止該等個人資料侵害事件的發生。

73. As usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration. These kinds of breaches are typically breaches of confidentiality, since the database is usually left intact, its content "merely" copied for further use. The quantity of data affected is usually also low or medium. In this particular case no special categories of personal data were affected, the employee only needed the contact information of clients to enable him to get in touch with them after leaving the company. Therefore, the data concerned is not sensitive.
與上列案例相同，於風險評估過程中，要考量到個人資料侵害事件的類型及受影響個人資料之性質、敏感性及數量。此類事件一般屬機密性之侵害事件，因為資料庫的完整性沒有受到影響，其內容「僅」遭到複製及進一步使用。受影響之資料數量一般屬低、中程度。於本案例中，沒有特種個資受到影響，該員工僅需要客戶聯絡資訊供其離職後聯繫之用。因此，受影響資料並非敏感性資料。

74. Although the only goal of the ex-employee that maliciously copied the data may be limited to gaining the contact information of the company's clientele for his own commercial purposes, the controller is not in a position to consider the risk for the affected data subjects to be low, since the controller does not have any kind of reassurance on the intentions of the employee. Thus, while the consequences of the breach might be limited to the exposure to uncalled-for self-marketing of the ex-employee, further and more grave abuse of the stolen data is not ruled out, depending on the purpose of the processing put in place by the ex-employee[25].
雖然該前員工惡意複製資料的唯一目標，可能僅限於為自身商業目的取得公司客戶的聯絡資訊，但控管者無法據此認定受影響當事人所面臨的風險很低，因為控管者無法保證該前員工的確切意圖為何。因此，雖然此個人資料侵害事件的後果可能僅限於前員工主動向該等客戶行銷，仍無法排除進一步及更嚴重地濫用遭竊資料的可能性，端視該前員工運用資料之目的而定[25]。

4.1.2. CASE No. 08 – Mitigation and obligations
案例 08－緩解措施及義務

75. The mitigation of the adverse effects of the breach in the above case is difficult. It might need to involve immediate legal action to prevent the former employee from abusing and disseminating the data any further. As a next step, the avoidance of similar future situations should be the goal. The controller might try to order the ex-employee to stop using the data, but the success of this action is dubious at best. Appropriate technical measures such as the impossibility of copying or downloading data to removable devices may help.
於本案例中，很難緩解個人資料侵害事件之不利影響，可能需要立即採取法律行動來防止前員工進一步濫用及傳播資料。下一步則應以避免未來發生類似事件為目標。控管者可以嘗試要求前員工停止使用資料，但此要求成功可能性不高。採取適當的技術上措施（例如：禁止複製或下載資料至行動裝置）可能會有幫助。

76. There is no "one-size fits-all" solution to these kinds of cases, but a systematic approach may help to prevent them. For example, the company may consider – when possible - withdrawing certain forms of access from employees who have signalled their intention to quit or implementing access logs so that unwanted access can be logged and flagged. The contract signed with employees should include clauses that prohibit such actions.
此等事件並沒有一體適用的解決方案，但採取系統性的作法可能有助於防止此等事件。例如，公司可以考慮（在可能的情況下）針對已提出辭職想

---

[25] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

法的員工，限制其存取資料的特定權限，或備置資料存取日誌，俾以記錄及發現不必要的資料存取。與員工簽署的合約中應納入禁止該等行為之條款。

77. All in all, as the given breach will not result in a high risk to the rights and freedoms of natural persons, a notification to the SA will suffice. However, the information to the data subjects might be beneficial for the data controller too, since it might be better that they hear from the company about the data leak rather than from the ex-employee who tries to contact them. Data breach documentation in accordance with Article 33 (5) is a legal obligation.
總歸而言，由於此個人資料侵害事件不會對自然人之權利及自由造成高風險，因此僅須通報監管機關。然而，向當事人提供資訊可能對資料控管者也有益處，因為由公司主動將資料外洩的情況告知客戶，應比客戶從與其聯繫的前員工處得知較為理想。依據第 33 條第 5 項規定，記錄個人資料侵害事件係一項法律義務。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	X

4.2. CASE No. 09: Accidental transmission of data to a trusted third party
案例 09：意外將資料傳輸予可信賴之第三方

An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data

controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the breach.
一名保險代理人發現，因他人透過電子郵件傳送給他的Excel檔案中有設置錯誤，他居然能夠存取非屬於他負責範圍的二十幾名客戶的相關資訊。他受職業保密義務所拘束，且為電子郵件的唯一收件者。依資料控管者及保險代理人間之安排，代理人有義務立即向資料控管者通報個資侵害事件，不得無故遲延。因此，該代理人立即通知控管者此錯誤設置，控管者於修正檔案後重新寄送郵件，並要求該代理人刪除原始郵件。依據上述安排，代理人必須出具書面聲明確認刪除，代理人亦已出具聲明。代理人所取得的資訊不包括特種個資，僅有聯絡資訊及關於保險本身資料（保險類型、金額）。在分析受個人資料侵害事件影響之個人資料後，資料控管者沒有發現個人或資料控管者方面有任何可能左右個人資料侵害事件之影響程度的特殊情事。

4.2.1. CASE No. 09 – Prior measures and risk assessment
案例 09－事前措施及風險評估

78. Here the breach does not derive from an intentional action of an employee, but from an unintentional human error caused by inattentiveness. These kinds of breaches may be avoided or decreased in frequency by a) enforcing training, education and awareness programs where employees gain a better understanding of the importance of personal data protection, b) reducing file exchange through e-mail, instead using dedicated systems for processing customer data for example, c) double checking files before sending, d) separating the creation and sending of files.
於本案例中，個人資料侵害事件並非始自員工的故意行為，而係因不注意而造成的非故意人為錯誤。這類個人資料侵害事件可以透過以下方式避免或降低頻率：a) 實施訓練、教育及宣導計畫，讓員工更深入瞭解個人資料保護的重要性；b) 減少透過電子郵件交換文件，改採（包括但不限於）專用系統來運用客戶資料；c) 在傳送郵件前再次檢查文件；d) 將創建文件及傳送文件的作業進行區隔。

79. This data breach concerns only the confidentiality of the data, and the integrity and the accessibility thereof are left intact. The data breach only concerned about two dozen costumers, hence the quantity of data affected can be considered as low. Furthermore, the personal data affected does not contain any sensitive data. The fact that the data processor immediately contacted the data controller after becoming aware of the data breach can be considered a risk mitigating factor.

(The possibility of data having been sent to other insurance agents should also be evaluated and, if confirmed, proper measures should be taken.) Due to the appropriate steps taken after the data breach, it will probably not have any impact on the data subjects' rights and freedoms.
這起個人資料侵害事件僅涉及資料之機密性，其完整性及可存取性均未受到影響，且只有二十幾名客戶受到影響。因此，受影響的資料量可以說是很低。此外，受影響之個人資料並不包含任何敏感性資料。資料受託運用者於意識到個人資料侵害事件後立即聯絡資訊控管者，這可被認為是緩解風險之因素。（亦應評估資料被發送給其他保險代理人的可能性；若可能，則應採取適當措施）。由於在發生個人資料侵害事件後採取適當措施，可能不會對當事人之權利及自由產生任何影響。

80. The combination of the low number of individuals affected, the immediate detection of the breach and the measures taken to have its effects minimized make this particular case no risk.
受影響之當事人不多，立即發現並採取措施將其影響降至最低，該等因素綜合起來使本案沒有風險。

4.2.2. CASE No. 09 – Mitigation and obligations
案例 09－緩解措施及義務

81. Moreover, other risk mitigating circumstances are at play as well: the agent is bound by professional secrecy; he himself reported the problem to the controller; and he deleted the file upon request. Raising awareness and possibly including additional steps in checking documents involving personal data will probably help avoid similar cases in the future.
此外，其他緩解風險的情事亦有發揮作用：代理人受職業保密義務之拘束，並主動向控管者通報問題；代理人應要求刪除文件。持續宣導並在可能的情況下實施額外步驟（如檢查涉及個人資料的文件），可能有助於避免未來發生類似事件。

82. Besides documenting the breach in accordance with Article 33 (5), there is no need for any other action.
除依據第 33 條第 5 項記錄個人資料侵害事件外，毋須採取任何其他行動。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

4.3. Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources
防範內部人為風險來源/緩解其影響之組織上及技術上措施

83. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.
依據本案件之獨有特點，綜合採取以下措施，應有助於降低類似個人資料侵害事件再次發生的機會。

84. Advisable measures:
建議之措施：

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下列措施並非詳盡完整清單。列舉下列措施之用意在於提供防範構思及可能的解決方案。因資料運用活動性質不同，控管者應自行決定最適合特定情況的措施。）

- Periodic implementation of training, education and awareness programs for employees on their privacy and security obligations and the detection and reporting of threats to the security of personal data[26]. Develop an awareness program to remind employees of the most commons errors leading to personal data breaches and how to avoid them.
定期對員工實施訓練、教育及宣導計畫，使其瞭解其隱私權及安全義務，偵測及通報對個人資料安全之威脅[26]。訂定宣導計畫，提醒員工注意會造成個人資料侵害事件之最常見錯誤及如何避免該等錯誤。

- Establishment of robust and effective data protection and privacy practices, procedures and systems[27].
建立健全有效的資料保護及隱私權實踐、程序及系統[27]。

- Evaluation of privacy practices, procedures and systems to ensure continued effectiveness[28].

---

26 Section 2) subsection (i) of the Resolution to address the role of human error in personal data breaches.
資料保護及隱私權專員國際會議決議之第 2 條第 i 項，關於人為錯誤於個資侵害事件中所扮演的角色。

27 Section 2) subsection (ii) of the Resolution to address the role of human error in personal data breaches.
資料保護及隱私權專員國際會議決議之第 2 條第 ii 項，關於人為錯誤於個資侵害事件中所扮演的角色。

28 Section 2) subsection (iii) of the Resolution to address the role of human error in personal data breaches.
資料保護及隱私權專員國際會議決議之第 2 條第 iii 項，關於人為錯誤於個資侵害事件中所扮演的角色。

對隱私權實踐、程序及系統進行評估，以確保其持續有效[28]。

- Making proper access control policies and forcing users to follow the rules.
  訂定適當之存取權限控管政策，要求使用者遵守規則。
- Implementing techniques to force user authentication when accessing sensitive personal data.
  實施相關技術，要求使用者在存取敏感性個人資料時必須進行驗證。
- Disabling the company related account of the user as soon as the person leaves the company.
  使用者一旦離開公司，就立即停用該使用者之公司相關帳戶。
- Checking unusual dataflow between the file server and employee workstations.
  檢查檔案伺服器及員工工作站之間的異常資料流動。
- Setting up I/O interface security in the BIOS or through the use of software controlling the use of computer interfaces (lock or unlock e. g. USB/CD/DVD etc.).
  於 BIOS 中設置 I/O 介面安全機制，或透過使用軟體控制電腦介面之使用（例如鎖定或解鎖 USB/CD/DVD 等）。
- Reviewing employees' access policy (e.g. logging access to sensitive data and requiring the user to input a business reason, so that this is available for audits).
  檢視員工之資料存取政策（例如，針對敏感性資料之存取備置紀錄，並要求使用者輸入業務事由以供查核）。
- Disabling open cloud services.
  禁用開放的雲端服務。
- Forbidding and preventing access to known open mail services.
  禁止及防止存取已知的公開郵件服務。
- Disabling print screen function in OS.
  禁用作業系統中的螢幕截圖功能。
- Enforcing a clean desk policy.
  簽署辦公桌面淨空政策。
- Automated locking all computers after a certain amount of time of inactivity.
  於閒置一段時間後自動鎖定電腦。
- Use mechanisms (e.g. (wireless) token to log on/open locked accounts) for fast user switches in shared environments.
  採用相關機制（例如（無線）憑證登錄/開啟鎖定帳戶）以於共用環境中快速切換使用者。
- Use of dedicated systems for managing personal data that apply appropriate

access control mechanisms and that prevent human mistake, such as sending of communications to the wrong subject. The use of spreadsheets and other office documents is not an appropriate means to manage client data.
採用專用系統來管理個人資料，部署適當之存取權限控管機制，並防止人為錯誤（例如：將訊息發送給錯誤對象）。使用電子試算表及其他辦公文件並非管理客戶資料的適當方法。

5. LOST OR STOLEN DEVICES AND PAPER DOCUMENTS
滅失或遭竊之裝置及紙本文件

85. A frequent type of case is the loss or theft of portable devices. In these cases, the controller has to take into consideration the circumstances of the processing operation, such as the type of data stored on the device, as well as the supporting assets, and the measures taken prior to the breach to ensure an appropriate level of security. All of these elements affect the potential impacts of the data breach. The risk assessment might be difficult, as the device is no longer available.
可攜帶式裝置之滅失或遭竊屬常見的個人資料侵害事件類型。於該等情況下，控管者必須考量到資料運用作業的相關情況（例如：儲存在該裝置上之資料類型）及輔助資源，以及於個人資料侵害事件發生前已採取的措施，以確保適當之安全水準。所有該等因素均會影響個人資料侵害事件之潛在影響。風險評估可能很難執行，因為裝置已不存在。

86. These kinds of breaches can be always classified as breaches of confidentiality. However, if there is no backup for the stolen database, then the breach type can also be breach of availability and breach of integrity.
該等類型之個人資料侵害事件均可被歸類為機密性侵害事件。然而，若遭竊之資料庫沒有備份，則亦屬可用性及完整性之侵害事件。

87. The scenarios bellow demonstrate how the above mentioned circumstances influence the likelihood and severity of the data breach.
下列案例呈現上述情事會如何左右個人資料侵害事件之可能性及重大程度。

5.1. CASE No. 10: Stolen material storing encrypted personal data
案例 10：存有經加密個人資料之裝置遭竊

During a break-in into a children's day-care centre, two tablets were stolen. The tablets contained an app which held personal data about the children attending the day-care centre. Name, date of birth, personal data about the education of the children were concerned. Both the encrypted tablets which were turned off at the time of the break-in, and the app were protected by a strong password. Back-up data was effectively and readily available to the controller. After

becoming aware of the break-in, the day-care remotely issued a command to wipe the tablets shortly after the discovery of the break-in.
一家托兒所遭小偷，有兩台平板電腦遭竊。該等平板電腦中的一個應用程式內存有托兒所小朋友的個人資料，涉及姓名、出生日期及教育相關資料。兩台經加密的平板電腦在遭竊時均為關閉的狀態，而該應用程式也受到高強度密碼所保護。控管者的備份資料是有效且隨時可用的。在發現遭小偷後，托兒所很快就透過遠端操作刪除該等平板電腦裡的資料。

5.1.1. CASE No. 10 - Prior measures and risk assessment
案例 10－事前措施及風險評估

88. In this particular case the data controller took adequate measures to prevent and mitigate the impacts of a potential data breach by using device encryption, introducing adequate password protection and securing back-up of the data stored on the tablets. (A list of advisable measures is to be found in section 5.7).
於本案例中，資料控管者採取充分措施，透過將裝置進行加密、部署適當的密碼保護並就平板電腦中儲存的資料進行備份，來防止及緩解潛在個人資料侵害事件之影響。（建議措施清單請參考第 5.7 段）。

89. After becoming aware of a breach, the data controller should assess the risk source, the systems supporting the data processing, the type of personal data involved and the potential impacts of the data breach on the concerned individuals. The data breach described above would have concerned confidentiality, availability and integrity of the concerned data, however due to the appropriate proceedings of the data controller prior and after the data breach none of these occurred.
在發現個人資料侵害事件後，資料控管者應評估風險來源、支援資料運用之系統、涉及之個人資料類型及個人資料侵害事件對相關個人的潛在影響。上述個人資料侵害事件會涉及到相關資料之機密性、可用性及完整性，但由於資料控管者在個人資料侵害事件之前及之後均採取適當程序，相關資料之機密性、可用性及完整性均未遭到影響。

5.1.2. CASE No. 10 – Mitigation and obligations
案例 10－緩解措施及義務

90. The confidentiality of the personal data on the devices was not compromised due to the strong password protection on both the tablets and the apps. The tablets were set up in such a way that setting a password also means that the data on the device is encrypted. This was further enhanced by the controller's action to attempt to remotely wipe everything from the stolen devices.

由於平板電腦及應用程式均有高強度密碼保護，裝置上個人資料之機密性並未受到影響。該等平板電腦的設置方式，是在設置密碼的同時也就資料進行加密。控管者試圖透過遠端操作刪除遭竊設備上的所有資料，亦進一步提升了安全性。

91. Due to the measures taken, the confidentiality of the data was kept intact too. Furthermore, the backup ensured the continuous availability of the personal data, hence no potential negative impact could have occurred.
由於控管者採取了上述措施，資料之機密性得以獲得保障。此外，備份資料亦確保個人資料之持續可用性，因此並未發生任何潛在不利影響。

92. Due to these facts, the above described data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33 (5).
基於上述，此個人資料侵害事件不太可能對當事人之權利及自由造成風險，因此毋須通報監管機關或通知相關當事人。然而，依據第 33 條第 5 項規定，仍須記錄此個人資料侵害事件。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

5.2. CASE No. 11: Stolen material storing non-encrypted personal data
案例 11：存有未加密個人資料之裝置遭竊

The electronic notebook device of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers. Due to the unavailability of the stolen device it was not possible to identify if other categories of personal data were also affected. The access to the notebook's hard drive was not protected by any password. Personal data could be restored from daily backups available.
一家服務供應商員工的筆記型電腦遭竊，其中存有超過 10 萬名客戶的姓名、性別、地址及出生日期。由於裝置已遭竊，因此無法確定其他類別的個人資料是否也受到影響。對該筆電硬碟之存取並未設定任何密碼保護。但可依據每日備份資料還原個人資料。

5.2.1. CASE No. 11 - Prior measures and risk assessment

案例 11－事前措施及風險評估

93. No prior safety measures were taken by the data controller, hence the personal data stored on the stolen notebook was easily accessible for the thief or any other person coming into possession of the device thereafter.
資料控管者事前並未採取任何安全措施，因此儲存在遭竊筆電中的個人資料很容易遭竊賊或後續取得該裝置的任何其他人存取。

94. This data breach concerns the confidentiality of the data stored on the stolen device.
此個人資料侵害事件會影響遭竊設備上所儲存資料之機密性。

95. The notebook containing the personal data was vulnerable in this case because it did not possess any password protection or encryption. The lack of basic security measures enhances the risk level for the affected data subjects. Furthermore, the identification of the concerned data subjects is also problematic, which also increases the severity of the breach. The considerable number of concerned individuals increases the risk, nevertheless, no special categories of personal data were concerned in the data breach.
於本案例中，存有個人資料的筆電相當脆弱，因為其不具備任何密碼保護或加密功能。缺乏基本安全措施提高了受影響當事人之風險程度。此外，因無法識別相關當事人，也提升了此個人資料侵害事件的重大性。受影響人數眾多也提高了風險；雖然如此，此個人資料侵害事件並未涉及特種個資。

96. During the risk assessment[29] the controller should take into consideration the potential consequences and adverse effects of the confidentiality breach. As a result of the breach the concerned data subjects may suffer identity fraud relying on the data available on the stolen device, so risk is considered to be high.
於風險評估期間[29]，控管者應考量機密性遭侵害的潛在後果及不利影響。由於發生此個人資料侵害事件，相關當事人可能會因為遭竊裝置上的資料而遭受身分詐欺，所以此事件被認為屬高風險。

5.2.2. CASE No. 11 – Mitigation and obligations
案例 11－緩解措施及義務

97. Turning on device encryption and the use of strong password protection of the stored database could have prevented the data breach to result in a risk to the rights and freedoms of the data subjects.
運用裝置加密及對儲存資料庫採用高強度密碼保護，可以防止個人資料侵

---

[29] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

害事件對當事人之權利及自由造成風險。

98. Due to these circumstances the notification of the SA is required, the notification of the concerned data subjects is also necessary.
基於上述情況，有必要通報監管機關，也必須通知相關當事人。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

5.3. CASE No. 12: Stolen paper files with sensitive data
案例 12：含有敏感性資料之紙本文件遭竊

A paper log book was stolen from a drug addiction rehab facility. The book contained basic identity and health data of the patients admitted to the rehab facility. The data was only stored on paper and no backup was available to the doctors treating the patients. The book was not stored in a locked drawer or a room, the data controller had neither an access control regime nor any other safeguarding measure for the paper documentation.
一家勒戒所的紙本日誌本遭竊，其中包含該勒戒所收治病患的基本身分資料及健康資料。該等資料僅記錄於紙本，治療病患的醫師沒有備份。該日誌本並未存放在上鎖的抽屜或房間裡，資料控管者既沒有建立存取權限控管制度，亦沒有對紙本文件採取任何其他保護措施。

5.3.1. CASE No. 12 – Prior measures and risk assessment
案例 12－事前措施及風險評估

99. No prior safety measures were taken by the data controller, hence the personal data stored in this book was easily accessible for the person who found it. Moreover, the nature of the personal data stored in the book makes the lack of backup data a very serious risk factor.
資料控管者事前並未採取任何安全措施，因此儲存在此日誌本中的個人資料很容易被持有此文件者存取。此外，有鑑於本文件中個人資料之性質，使得缺乏備份資料成為非常重大的風險因素。

100. This case serves as an example for a high-risk data breach. Due to the failure of appropriate safety precautions, sensitive health data pursuant to Article 9 (1) GDPR was lost. Since in this case a special category of personal data was concerned, the potential risks to the concerned data subjects was increased, which

should be also taken into consideration by the controller assessing the risk[30].
本案為高風險個人資料侵害事件案例。由於未採取適當的安全預防措施，GDPR 第 9 條第 1 項所載之敏感健康資料因此滅失。由於本案涉及特種個資，相關當事人之潛在風險增加，這也是控管者於評估風險時所必須考量的因素[30]。

101. This breach concerns the confidentiality, availability and integrity of the concerned personal data. As a result of the breach, medical secrecy is broken and unauthorized third parties may gain access to the patients' private medical information, what may have severe impact on the patient's personal life. The availability breach may also disturb the continuity of the patients' treatment. Since the modification/deletion of parts of the book's content may not be excluded, the integrity of the personal data is also compromised.
此個人資料侵害事件涉及影響相關個人資料之機密性、可用性及完整性。由於此個人資料侵害事件，醫療機密性會受到侵害，未經授權之第三方可能取得病患的私人醫療資訊，這可能對病患的個人生活產生重大影響。可用性之侵害也可能干擾病患治療之連續性。由於該紀錄中部分內容可能遭到變更/刪除，個人資料的完整性也有可能會受到影響。

5.3.2. CASE No. 12 – Mitigation and obligations
案例 12－緩解措施及義務

102. During the assessment of the safeguarding measures the type of the supporting asset should be considered as well. Since the patient log book was a physical document, its safeguarding should have been organized differently than that of an electronic device. The pseudonymisation of the patients' names, the storage of the book in a safeguarded premises and in a locked drawer or a room, and proper access control with authentication when accessing it could have prevented the data breach.
於評估保護措施的過程中，亦應考量輔助資源之類型。由於病患日誌本是一份實體文件，其保護工作的處理方式應與電子裝置有所不同。將病患姓名進行假名化、將日誌本存放於受保護的場所及上鎖的抽屜或房間中，訂定適當的存取權限控管及驗證機制，均可防止個人資料侵害事件。

103. The above described data breach may severely impact the concerned data subjects; hence the notification of the SA and communication of the breach to the concerned data subjects is mandatory.
此個人資料侵害事件可能會對相關當事人造成重大影響，因此必須將此個人資料侵害事件通報監管機關並通知相關當事人。

---

30 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

Actions necessary based on the identified risks 依據經識別風險所必須採取的行動		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

5.4. Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices
防範裝置滅失或遭竊/緩解其影響之組織上及技術上措施

104. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.
依據本案件之獨有特點，綜合採取以下措施，應有助於降低類似個人資料侵害事件再次發生的機會。

105. Advisable measures:
建議之措施：

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下列措施並非詳盡完整清單。列舉下列措施之用意在於提供防範構思及可能的解決方案。因資料運用活動性質不同，控管者應自行決定最適合特定情況的措施。）

- Turn on device's encryption (such as Bitlocker, Veracrypt or DM-Crypt).
開啟裝置之加密功能（如 Bitlocker、Veracrypt 或 DM-Crypt）。
- Use passcode/password on all devices. Encrypt all mobile electronic devices in a way that requires the input of a complex password for decryption.
於所有裝置上使用密碼/金鑰。對所有行動裝置進行加密，要求輸入複雜密碼始得解密。
- Use multi-factor authentication.
採用多因素驗證機制。
- Turn on the functionalities of highly mobile devices that allow them to be located in case of loss or misplacement.
開啟高度行動裝置之定位功能，使其於遺失或誤置的情況下能夠被定位。
- Use MDM (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices.

使用 MDM（行動裝置管理）軟體/應用程式及定位功能。使用防窺片。關閉任何無人看管的裝置。

- If possible and appropriate to the data processing in question, save personal data not on a mobile device, but on a central back-end server.
  若可能且於適合相關資料運用的情況下，不要把個人資料儲存在行動裝置上，而應儲存在中央後端伺服器上。
- If the workstation is connected to the corporate LAN, do an automatic backup from the work folders provided it is unavoidable that personal data is stored there
  若工作站連接至企業局部區域網絡（LAN），且個人資料必須儲存於該處，則應自工作資料夾中進行自動備份。
- Use a secure VPN (e.g. which requires a separate second factor authentication key for the establishment of a secure connection) to connect mobile devices to back-end servers.
  採用安全的虛擬私人網絡（VPN）（例如，需要獨立第二要素驗證金鑰來建立安全連接）來連接行動裝置及後端伺服器。
- Provide physical locks to employees in order to enable them to physically secure mobile devices they use while they remain unattended.
  為員工提供實體/物理鎖，使其能夠在無人看管裝置的情況下，對其使用之行動裝置進行實體/物理保護。
- Proper regulation of device usage outside the company.
  針對於公司場所外使用裝置訂定適當規範。
- Proper regulation of device usage inside the company.
  針對於公司場所內使用裝置訂定適當規範。
- Use MDM (Mobile Devices Management) software/app and enable the remote wipe function.
  使用 MDM（行動裝置管理）軟體/應用程式並啟用遠端刪除功能。
- Use centralised device management with minimum rights for the end users to install software.
  採用中心化的裝置管理，向終端使用者授予使其得以安裝軟體的最低權限。
- Install physical access controls.
  部署實體/物理存取權限控管措施。
- Avoid storing sensitive information in mobile devices or hard drives. If there is need to access the company's internal system, secure channels should be used such as previously stated.

避免將敏感性資訊儲存在行動裝置或硬碟中。若需要存取公司內部系統，應透過上述安全管道。

6. MISPOSTAL
郵遞錯誤

106. The risk source is an internal human error in this case as well, but here no malicious action led to the breach. It is the result of inattentiveness. Little can be undertaken by the controller after it happened, so prevention is even more important in these cases than in other breach types.
於本案例中，風險來源同樣是內部人為錯誤，但個人資料侵害事件並非是惡意行動所造成，而是不注意的結果。於事件發生後，控管者能夠採取的措施很少，因此於此等情況下，採取預防措施比其他類型事項更加重要。

6.1. CASE No. 13: Postal mail mistake
案例 13：郵遞錯誤

Two orders for shoes were packed by a retail company. Due to human error two packing bills were mixed up with the result that both products and the relevant packing bills were sent to the wrong person. This means that the two customers got each other's orders, including the packing bills containing the personal data. After becoming aware of the breach the data controller recalled the orders and sent them to the right recipients.
一家零售公司已打包好兩張鞋履訂單包裹準備出貨。由於人為錯誤，兩張裝箱單被搞混了，結果兩個包裹及相關的裝箱單都被寄給錯誤的收件人，亦即這兩個客戶收到了對方的包裹，且其中含有記載對方個人資料之裝箱單。在知悉此個人資料侵害事件後，資料控管者召回該等包裹，並將正確包裹寄送予正確的收件人。

6.1.1. CASE No. 13 - Prior measures and risk assessment
案例 13－事前措施及風險評估

107. The bills contained the personal data required for a successful delivery (name, address, plus the item purchased and its price). It is important to identify how the human error could have happened in the first place, and if in any way, it could have been prevented. In the particular case describe the risk is low, since no special categories of personal data or other data whose abuse might lead to substantial negative effects were involved, the breach is not a result of a systemic error on the controller’s part and only two individuals are concerned. No negative effect on the individuals could be identified.

裝箱單中記載成功送貨所必須的個人資料（姓名、地址、購買商品及其價格）。首要任務是需判斷人為錯誤是如何發生，以及是否得以任何方式防止該錯誤。本案例所涉風險很低，因為不涉及特種個資，亦不涉及其他一旦遭濫用就可能導致重大不利影響的資料；此個人資料侵害事件並非係因控管者之系統錯誤所造成，且僅涉及兩個人，無法確定對該等個人造成不利影響。

6.1.2. CASE No. 13 – Mitigation and obligations
案例 13－緩解措施及義務

108. The controller should provide for a free return of the items and the accompanying bills, and it also should request the wrong recipients to destroy / delete all eventual copies of the bills containing the other person's personal data.
控管者應提供免費返還商品及隨附之裝箱單，亦應要求錯誤的收件人銷毀/刪除所有含有他方當事人個人資料之裝箱單。

109. Even if the breach itself does not pose a high risk to rights and freedoms of the affected individuals, and thus communication to the data subjects is not mandated by Article 34 GDPR, communication of the breach to them cannot be avoided, as their cooperation is needed to mitigate the risk.
因個人資料侵害事件本身並不會對受影響個人之權利及自由構成高風險，GDPR 第 34 條並未強制要求通知當事人，但因為需要當事人的配合以緩解事件風險，所以仍不可避免地必須向當事人通知此個人資料侵害事件。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

6.2. CASE No. 14: Highly confidential personal data sent by mail by mistake
案例 14：高度機密之個人資料遭誤寄

The employment department of a public administration office sent an e-mail message – about upcoming trainings - to the individuals registered in its system as jobseekers. By mistake, a document containing all these jobseekers' personal data (name, e-mail address, postal address, social security number) was attached to this e-mail. The number of affected individuals is more than 60000. Subsequently the office contacted all the recipients and asked them to delete the previous message and not to use the information contained in it.

公共行政辦公室的僱傭部門向於其系統中登記為求職者的個人發送了一封關於即將舉辦訓練課程的電子郵件。由於失誤，一份內含所有該等求職者個人資料（姓名、電子郵件地址、郵政地址、社會保險號碼）的檔案被檢附於此電子郵件中。受影響的人數超過 6 萬人。隨後，該辦公室聯絡所有收件人，要求其刪除該檔案且不要使用其中資訊。

6.2.1. CASE No. 14 - Prior measures and risk assessment
案例 14－事前措施及風險評估

110. Stricter rules should have been implemented for sending such messages. The introduction of additional control mechanisms need to be considered.
原本即應針對該等訊息之發送實施更嚴格的規範。應考量採取額外的控管機制。

111. The number of affected individuals is considerable, and the involvement of their social security number, along with other, more basic personal data, further increases the risk, which can be identified as high[31]. The eventual distribution of the data by any of the recipients cannot be contained by the controller.
受影響個人數量眾多，並涉及其社會安全號碼及其他更基本的個人資料，因此進一步提高風險；本事件因此可確認屬高風險 [31]。控管者無法控制任何收件人最終是否散布該等資料。

6.2.2. CASE No. 14 – Mitigation and obligations
案例 14－緩解措施及義務

112. As mentioned earlier, the means to effectively mitigate the risks of a similar breach, are limited. Though the controller asked for the deletion of the message, it cannot force the recipients to do so, and as a consequence, nor can it be certain that they comply with the request.

如前所述，有效緩解此類事件風險的手段相當有限。雖然控管者要求刪除資訊，但無法強迫收件人遵守，因此無法確定收件人是否確實遵守該要求。

113. The execution of all three below indicated actions should be self-evident in a case like this.
於此情況下，顯然必須採取下列三項行動。

Actions necessary based on the identified risks

[31] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

依據經識別風險所必須採取的行動		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

6.3. CASE No. 15: Personal data sent by mail by mistake
案例 15：個人資料遭誤寄

A list of participants on a course in Legal English which takes place in a hotel for 5 days is by mistake sent to 15 former participants of the course instead of the hotel. The list contains names, e-mail addresses and food preferences of the 15 participants. Only two participants have filled in their food preferences, stating that they are lactose intolerant. None of the participants have a protected identity. The controller discovers the mistake immediately after sending the list and informs the recipients of the mistake and asks them to delete the list.
一堂為期五日且將於某飯店舉辦的法律英語課程，本要將新生名單發送給該飯店，但卻誤將此名單發送給 15 名舊生。該名單內含 15 名新生的姓名、電子郵件地址及飲食偏好。僅有兩名學員有填寫飲食偏好（說明其有乳糖不耐症）。所有學員的身分資料均未受到保護。控管者在發送名單後立即發現此錯誤，並通知收件人此一錯誤，要求其刪除該名單。

6.3.1. CASE No. 15 - Prior measures and risk assessment
案例 15－事前措施及風險評估

114. Strict rules should have been implemented for sending of messages containing personal data. The introduction of additional control mechanisms need to be considered.
原本即應針對該等含有個人資料訊息之發送實施更嚴格的規範。應考量採取額外的控管機制。

115. The risks deriving from the nature, the sensitivity, the volume and the context of the personal data are low. The personal data includes sensitive data on food preferences of two of the participants. Even if the information that someone is lactose intolerant is health data, the risk that this data will be used in a detrimental way should be considered relatively low. While in the case of data concerning health it is usually assumed that the breach is likely to result in a high risk for the

data subject[32], at the same time in this particular case no risk can be identified that the breach will lead to physical, material or non-material damages of the data subject due to the unauthorised disclosure of lactose intolerance information. Contrary to some other food preferences, lactose intolerance can normally not be linked to any religious or philosophical beliefs. The quantity of the breached data and the number of affected data subjects is very low as well.
依據該等個人資料之性質、敏感性、數量及脈絡判斷，此事件之風險很低。個人資料包括兩名學員飲食偏好之敏感性資料。雖然對乳糖不耐症之資訊屬健康資料，但此資料被用於有害方式使用的風險相對較低。雖然涉及健康資料的情況一般會被認為會使當事人遭受高風險[32]，但於本案例中，此個人資料侵害事件應不會因未經授權揭露乳糖不耐症之資訊而導致當事人遭受人身、財物或非財物損害。相較於其他飲食偏好，乳糖不耐症通常無涉任何宗教或哲學信仰。遭揭露之資料數量及受影響當事人之數量亦非常少。

6.3.2. CASE No. 15 – Mitigation and obligations
案例 15－緩解措施及義務

116. In summary, it can be stated that the breach had no significant effect on the data subjects. The fact that the controller immediately contacted the recipients after becoming aware of the mistake can be considered as a mitigating factor.
綜上所述，此個人資料侵害事件對當事人並無重大影響。控管者於發現錯誤後立即與收件人聯絡，這一事實可以被認為是緩解影響的因素。

117. If an email is sent to an incorrect/unauthorised recipient, it is recommended that the data controller should Bcc a follow up email to the unintended recipients apologising, instructing that the offending email should be deleted, and advising recipients that they do not have the right to further use the email addresses identified to them.
若電子郵件被發送給錯誤/未經授權之收件人，建議資料控管者應隨即向錯誤之收件人發送電子郵件以表示歉意，請求刪除錯誤的電子郵件，並告知收件人其無權進一步使用其接獲之電子郵件地址。

118. Due to these facts this data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33(5).
基於上述，此個人資料侵害事件不太可能對當事人之權利及自由造成風險，因此毋須通報監管機關或通知相關當事人。然而，依據第 33 條第 5 項，此

---

[32] See Guidelines WP 250, p. 23.
請參考第 WP250 號指引，第 23 頁。

個人資料侵害事件仍須進行紀錄。

Actions necessary based on the identified risks 依據經識別風險所必須採取的行動		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	X	X

6.4. CASE No. 16: Postal mail mistake
案例 16：郵遞錯誤

An insurance group offers car insurances. To do this, it sends out regularly adjusted contribution policies by postal mail. In addition to the name and address of the policyholder, the letter contains the vehicle registration number without masked digits, the insurance rates of the current and next insurance year, the approximate annual mileage and the policyholder's date of birth. Health data according to Article 9 GDPR, payment data (bank details), economic and financial data are not included.
一家提供汽車保險的保險集團透過郵局定期發送經調整後的保費繳款單。除投保人之姓名及地址外，信中亦包含車輛牌照號碼（無遮蔽）、目前及下一保險年度之保險費率、每年之大致里程數及投保人之出生日期。GDPR 第 9 條所載之健康資料、付款資料（銀行資訊）、經濟及財務資料則未不包括在內。

Letters are packed by automated enveloping machines. Due to a mechanical error, two letters for different policyholders are inserted into one envelope and sent to one policyholder by letter post. The policyholder opens the letter at home and takes a look at his correctly delivered letter as well as at the incorrectly delivered letter from another policyholder.
該等信件係由自動信封機所包裝。由於機械錯誤，兩封給不同投保人的信函被裝進同一信封內，並透過信件郵寄予投保人。投保人打開信封後看到正確投遞給他的信函以及原應投遞給另一投保人的錯誤信函。

6.4.1. CASE No. 16 - Prior measures and risk assessment
案例 16－事前措施及風險評估

119. The incorrectly delivered letter contains the name, address, date of birth, unmasked vehicle registration number and the classification of the insurance rate of the current and the next year. The effects on the affected person are to be

regarded as medium, since information not publicly available such as the date of birth or unmasked vehicle registration numbers, and details about the increment in insurance rates are disclosed to the unauthorized recipient. The probability of misuse of this data is assessed to be between low and medium. However, while many recipients will probably dispose of the wrongly received letter in the garbage, in individual cases it cannot be completely ruled out that the letter will be posted in social networks or that the policyholder will be contacted.
這封錯誤的信件內含姓名、地址、出生日期、未遮蔽之車輛牌照號碼及本年度及下一年度之保險費率分類。當事人所受影響程度被認為屬中等，因為非公開資訊（如出生日期或未遮蔽之車輛牌照號碼，及關於保險費率增加之詳細資訊）遭揭露予未經授權之收件人。該等資料遭到濫用的機率被評估為於低等及中等之間。然而，雖然許多收件人可能會將收件人有誤的信件扔進垃圾桶，但於個別情況下，仍無法完全排除信件會被張貼到社群網站上或被用來聯繫保戶。

6.4.2. CASE No. 16 – Mitigation and obligations
案例 16－緩解措施及義務

120. The controller should have the original document returned at its own expense. The wrong recipient should also be informed that he/she may not misuse the information read.
控管者應自費退還原始文件，亦應告知錯誤的收件人不得濫用其因此取得之資訊。

121. It will probably never be possible to completely prevent a postal delivery error in a mass mailing using fully automated machines. However, in the event of an increased frequency, it is necessary to check whether the enveloping machines are set and maintained correctly enough, or if some other systemic issue leads to such a breach.
使用全自動機器大量發送郵件，可能永遠無法完全杜絕郵遞錯誤，但若頻率增加，有必要檢查信封機之設置及維護是否充分、正確，或是否有其他系統性問題導致此等事件。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	X

6.5. Organizational and technical measures for preventing / mitigating the impacts of mispostal

防範郵遞錯誤/緩解其影響之組織上及技術上措施

122. A combination of the below mentioned measures – applied depending on the unique features of the case should help to lower the chance of a similar breach reoccurring.
依據本案件之獨有特點，綜合採取以下措施，應有助於降低類似個人資料侵害事件再次發生的機會。

123. Advisable measures:
建議之措施：

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下列措施並非詳盡完整清單。列舉下列措施之用意在於提供防範構思及可能的解決方案。因資料運用活動性質不同，控管者應自行決定最適合特定情況的措施。）

- Setting exact standards – with no room for interpretation - for sending letters / e-mails.
針對信件/電子郵件之發送實施確切標準（不留彈性空間）。
- Adequate training for personnel on how to send letters / e-mails.
針對如何發送信件/電子郵件提供充分教育訓練。
- When sending e-mails to multiple recipients, they are listed in the 'bcc' field by default.
當向多名收件人發送電子郵件時，應預設將其郵件列於密件副本欄位中。
- Extra confirmation is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
在向多名收件人發送電子郵件，且其電子郵件並非列於密件副本欄位中時，需要進行反覆確認。
- Application of the four-eyes principle.
遵循「四眼原則」。
- Automatic addressing instead of manual, with data extracted from an available and up-to-date database; the automatic addressing system should be regularly reviewed to check for hidden errors and incorrect settings.
應採自動輸入地址而非手動輸入，而地址資料應自既有之最新資料庫中提取；應定期檢視自動輸入地址系統，檢查是否有隱藏的錯誤及不正確的設置。
- Application of message delay (e.g. the message can be deleted / edited within

a certain time period after clicking the press button).
採用訊息延遲發送機制（例如：訊息得於點擊發送按鈕後一定時間內被刪除/編輯）。

- Disabling autocomplete when typing in e-mail addresses.
於輸入電子郵件地址時停用自動完成功能。
- Awareness sessions on most common mistakes leading to a personal data breach.
針對會造成個人資料侵害事件之最常見錯誤進行宣導。
- Training sessions and manuals on how to handle incidents leading to a personal data breach and who to inform (involve DPO).
針對如何處理會造成個人資料侵害事故之情事及該告知哪些對象(包含個人資料保護官)辦理訓練課程並備置手冊。

7. OTHER CASES – SOCIAL ENGINEERING
其他案例－社交工程

7.1. CASE No. 17: Identity theft
案例 17：身分冒用

The contact centre of a telecommunication company receives a telephone call from someone that poses as a client. The supposed client demands the company to change the email address to which the billing information should be sent from there on. The worker of the contact centre validates the client's identity by asking for certain personal data, as defined by the procedures of the company. The caller correctly indicates the requested client's fiscal number and postal address (because he had access to these elements). After the validation, the operator makes the requested change and, from there on, the billing information is sent to the new email address. The procedure does not foresee any notification to the former email contact. The following month the legitimate client contacts the company, inquiring why he is not receiving billing to his email address, and denies any call from him demanding the change of the email contact. Later, the company realizes that the information has been sent to an illegitimate user and reverts the change.
一家電信公司的客服中心接到一通假冒客戶的來電；假冒客戶者要求該公司變更客戶的電子郵件地址，要求將帳單資訊發送至新地址。客服中心之工作人員透過詢問公司程序所定義之特定個人資料來驗證客戶身分。來電者正確地提供客戶之財務代碼及郵遞地址（因他已存取該等資

訊）。完成驗證後，客服人員進行其所要求之變更，自此，帳單資訊均被發送至新的電子郵件地址。此程序中並未要求將變更事實寄送至原電子信箱。真正的客戶於下一個月與該公司聯絡，詢問為什麼沒有收到電子郵件帳單，並否認他曾去電要求變更電子郵件。此公司後續發現該客戶之資訊被發送予非法使用者，因此還原變更。

7.1.1. CASE No. 17 - Risk assessment, mitigation and obligations
案例 17－風險評估、緩解及義務

124. This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk[33], as billing data can give information about the data subject's private life (e.g. habits, contacts) and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organisation or exploit further authentication measures in other organisations. Considering these risks, the "appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication.
此案例說明採取事前防範措施的重要性。從風險方面來看，此個人資料侵害事件涉及高度風險[33]，因帳單資料涉及當事人之私人生活資訊（例如：習慣、連絡人），並可能導致財物損失（例如：遭跟蹤，對人身完整性造成風險）。於此等事件中取得的個人資料亦得被用來接手該帳戶或利用該公司所設置的其他驗證措施。考量到該等風險，實施「適當」驗證措施應達相當高的標準，並取決於通過驗證後可利用的個人資料範圍。

125. As a result, both a notification to the SA and a communication to the data subject are needed from the controller.
因此，控管者必須通報監管機關亦應通知當事人。

126. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be the intended user by the use of publicly available information and information that they otherwise had access to.
原有的客戶驗證流程顯然必須依據此案例進行調整。用於驗證的方法顯然不足。惡意攻擊者能夠透過使用公開資訊及其他可存取之資訊來假裝成特定使用者。

127. The use of this type of static knowledge-based authentication (where the answer does not change, and where the information is not "secret" such as would be the

---

33 For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
關於「可能導致高風險」資料運用作業之指導，請參考註腳 10。

case with a password) is not recommended.
不建議使用此等以相關知識為基礎之靜態驗證機制（亦即，答案不會改變，且資訊並非「秘密」，如採用密碼的情況）。

128. Instead, the organisation should use a form of authentication which would result in a high degree of confidence that the authenticated user is the intended person, and not anyone else. The introduction of an out-of-band multi-factor authentication method would solve the problem, e.g. to verify the change demand, by sending a confirmation request to the former contact; or adding extra questions and requiring information only visible on the previous bills. It is the controller's responsibility to decide which measures to introduce, as it knows the details and requirements of its internal operation the best.
實則，該公司應採用能以高度正確的方式確認使用者確實為其本人的驗證機制；採用頻外多因素（out-of-band multi-factor）驗證方法可以解決此問題，例如，透過向先前連絡人發送確認請求來驗證變更需求，或增加額外問題並要求提供僅有在先前帳單上才能看到的資訊。決定採用哪些措施是控管者的責任，因為控管者最瞭解其內部運作之細節及要求。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓

7.2. CASE No. 18: Email exfiltration
案例 18：電子郵件外洩

A hypermarket chain detected, 3 months after its configuration, that some email accounts had been altered and rules created so that every email containing certain expressions (e.g. "invoice", "payment", "bank wiring", "credit card authentication", "bank account details") would be moved to an unused folder and also forwarded to an external email address. Also, by that time, a social engineering attack had already been performed, i.e., the attacker, posing as a supplier, had had that supplier bank account details altered into his own. Finally, by that time, several fake invoices had been sent that included the new bank account detail. The monitoring system of the email platform ended up giving an alert regarding the folders. The company was unable to detect how the attacker was able to gain access to the email accounts to begin with, but it supposed that

an infected email was to blame for giving access to the group of users in charge of the payments.
一家連鎖大賣場於系統建置完成 3 個月後發現，某些電子郵件帳戶遭到竄改並遭納入特定規則，使每封均含有特定字詞（例如：「發票」、「付款」、「銀行匯款」、「信用卡驗證」、「銀行帳戶資訊」等）之電子郵件均會被移至未使用之資料夾中，同時轉發至外部電子郵件地址。另外，該大賣場亦遭受過一次社交工程攻擊，亦即，攻擊者冒充供應商，將該供應商之銀行帳戶資訊改成攻擊者本身帳戶資料。攻擊者當時已發送出幾張包含新銀行帳戶資訊之假發票。電子郵件平台之監控系統最終發出關於該等資料夾之警報。該大賣場無法判斷攻擊者是如何進入電子郵件帳戶，但認為應是受感染的電子郵件造成攻擊者得以接觸到負責收款的使用者群組。

Due to the keyword-based forwarding of emails, the attacker received information on 99 employees: name and wage of a particular month regarding 89 data subjects; name, civil status, number of children, wage, work hours and remainder information on the salary receipt of 10 employees whose contracts were ended. The controller only notified the 10 employees belonging to the latter group.
由於該等電子郵件之轉發係以關鍵字為基礎，攻擊者取得 99 名員工的資訊：關於 89 名當事人之姓名及某月工資；10 名已離職員工之姓名、婚姻狀況、子女數量、工資、工作時間及剩餘工資領取資訊。控管者僅通知屬後者之 10 名員工。

7.2.1. CASE No. 18 - Risk assessment, mitigation and obligations
案例 18－風險評估、緩解及義務

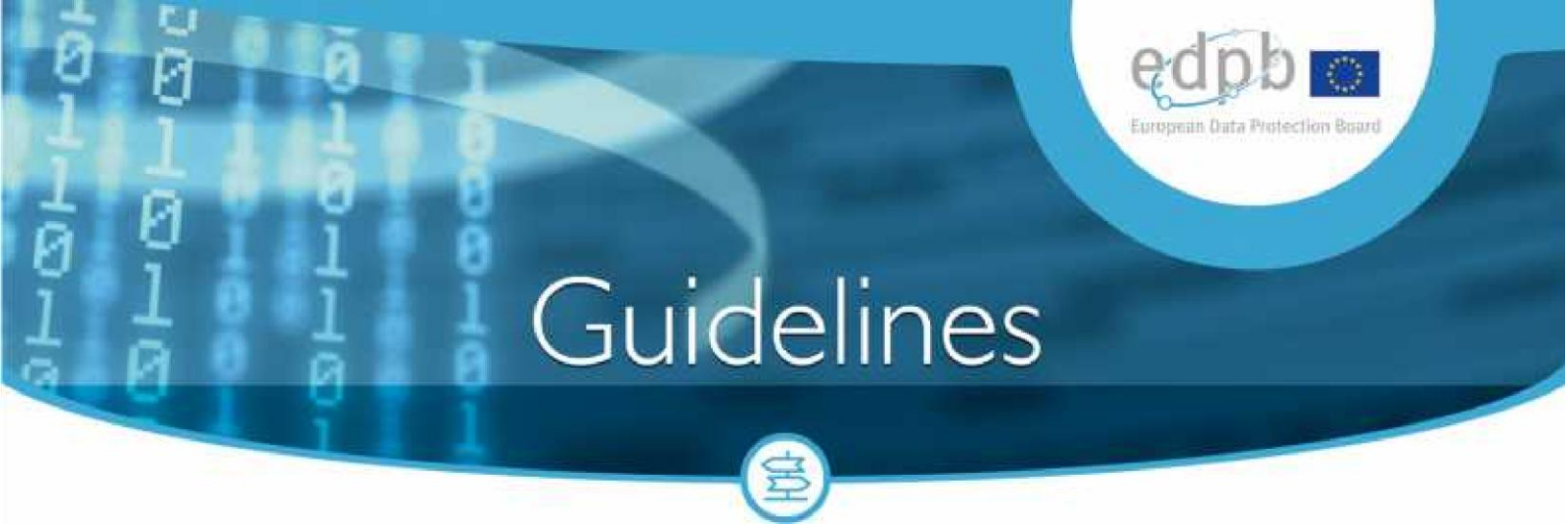
129. Even if the attacker was probably not aiming at collecting personal data, since the breach could lead to both material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud), or the data could be used to facilitate other attacks (e.g. phishing), the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Therefore the breach should be communicated to all 99 employees and not only to the 10 employees whose salary information was leaked.
即使攻擊者很可能並非以蒐集個人資料為目的，但由於資訊揭露可能導致財物（如財務損失）及非財物損失（如身分冒用或詐欺），或資料可能被用於從事其他攻擊（如網路釣魚），此個人資料侵害事件可能對自然人之權利及自由造成高風險。因此，應該向全數 99 名受影響員工通知該事件，

而非僅向工資資訊被揭露之 10 名員工發送通知。

130. After becoming aware of the breach, the controller forced a password change for the compromised accounts, blocked sending emails to the attacker's email account, notified the service provider of the email used by the attacker regarding his or her actions, removed the rules set by the attacker and refined the alerts of the monitoring system in order to give an alert as soon as an automatic rule is created. Alternatively, the controller could remove the right for users to set forwarding rules, needing the IT service team to do it only on request or it could introduce a policy that users should check and report on the rules set on their accounts once per week or more often, in areas handling financial data.
於發現個人資料侵害事件後，控管者強制變更遭攻擊帳戶之密碼，阻止向攻擊者之電子郵件帳戶發送電子郵件，將攻擊者之行為通知其電子郵件服務供應商，刪除攻擊者設置之規則，並改善監控系統之警報，俾以於自動規則創建後立即發出警報。另外，控管者可以取消使用者設置轉發規則之權利，要求資訊科技服務團隊僅得依據公司要求設置規則，或可規定使用者應每週（或更頻繁，若涉及財務資料之處理）檢查及通報其帳戶上所設置之規則。

131. The fact that a breach could happen and go undetected for so long and the fact that, in a longer time, social engineering could have been used for altering more data, highlighted significant problems in the controller's IT security system. These should be addressed without delay, like emphasizing automation reviews and change controls, incident detection and response measures. Controllers handling sensitive data, financial information, etc. have a larger responsibility in terms of providing adequate data security.
此個人資料侵害事件有可能發生且長時間沒有被發現，社交工程可能利用更長時間來變更更多資料之事實，顯示出控管者之資訊科技安全系統中存在重大問題。該等問題應該立即解決，例如：強化自動化檢查及變更控制、事故偵測及應變措施等。處理敏感性資料、金融資訊等之控管者，在確保資料安全方面肩負更大的責任。

Actions necessary based on the identified risks **依據經識別風險所必須採取的行動**		
Internal documentation 備置內部紀錄	Notification to SA 通報監管機關	Communication to data subjects 通知當事人
✓	✓	✓



Guidelines 07/2020 on the concepts of controller and processor in the GDPR
Version 2.1
Adopted on 07 July 2021

一般資料保護規則（GDPR）的控管者與受託運用者概念之指引07/2020

第2.1版

2021年7月7日通過

Version history
版本歷程

Version 2.1 第 2.1 版	20 September 2022 2022 年 9 月 20 日	Minor corrections 微幅修正。
Version 2.0 第 2.0 版	7 July 2021 2021 年 7 月 7 日	Adoption of the Guidelines after public consultation 經徵詢公眾意見後通過本指引。
Version 1.0 第 1.0 版	2 September 2020 2022 年 9 月 2 日	Adoption of the Guidelines for public consultation 徵詢公眾意見通過本指引。

EXECUTIVE SUMMARY
摘要

The concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The precise meaning of these concepts and the criteria for their correct interpretation must be sufficiently clear and consistent throughout the European Economic Area (EEA).
控管者、共同控管者和受託運用者的概念，在適用一般資料保護規則2016/679（GDRP）的規定時扮演關鍵角色，因為這些概念決定誰負責遵守不同的資料保護規定和當事人在實務上如何行使他們的權利。這些概念的確切意思和正確解釋標準必須在整個歐洲經濟區（EEA）都夠清楚且一致。

The concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law.
控管者、共同控管者和受託運用者的概念乃依據這些人的實際角色來分配責任，因此是功能性概念，這幾個概念應主要依據歐盟的資料保護法來解釋，因此是自主性概念。

Controller
控管者

In principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.
原則上，能擔任控管者角色的實體種類沒有限制，但實務上，通常是組織而不是組織內的個人（例如，執行長、員工或董事會成員）擔任控管者。

A controller is a body that *decides* certain key elements of the processing. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. Certain processing activities can be seen as naturally attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members). In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.
控管者決定資料運用的某些關鍵要素。控管者身分可由法律界定，或依據個案事實或情況的分析。某些運用活動可認為是自然附加於某個實體角色（僱主對於員工、出版社對於訂戶，或協會對於會員）。雖然不是所有情況

都能透過合約條款決定控管者，但在很多情況下，合約條款有助於識別控管者。

A controller determines the purposes and means of the processing, i.e. the *why* and *how* of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means") can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.
控管者決定資料運用的目的和方法，亦即，為何及如何運用。控管者必須決定目的和方法。但執行上有些比較實務的面向（「非必要方式」）可以留給受託運用者。控管者不需要能實際接觸正在運用的個人資料才有資格稱為控管者。

Joint controllers
共同控管者

The qualification as joint controllers may arise where more than one actor is involved in the processing. The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a *common decision* taken by two or more entities or result from *converging decisions* by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.
共同控管者的資格可能因運用過程有不止一位行為人參與而產生。GDRP 引進共同控管者的明確規定，並設定規範他們關係的架構。共同控管身分存在的首要標準是二個以上實體共同參與決定運用行動的目的和方法。共同參與可以採二個以上實體共同決定的形式，或來自二個以上實體的一致決定，這些決定彼此互補且係運用所必需，因此，它們對決定運用的目的和方法有實質影響。一個重要的標準是，沒有雙方的參與就無法運用，每一方的運用是無法分開的，亦即，緊密連結。共同參與必須包含決定目的及決定方法。

Processor
受託運用者

A processor is a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller's behalf.
受託運用者是代表控管者運用個人資料的自然人或法人、公務機關、機構或其他實體。有資格成為受託運用者的二個基本條件是：它和控管者是不同的實體，以及它代表控管者運用個人資料。

The processor must not process the data otherwise than according to the controller's instructions. The controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means. A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.
受託運用者除了依據控管者指示外，受託運用者不得運用資料。控管者的指示可以在某種程度上給予受託運用者裁量空間，允許受託運用者以最能符合控管者利益的方式選擇最合適的科技上和組織上方法。然而，一旦受託運用者超出控管者的指示，自行決定其運用目的和方法，它就違反了 GDPR 規定。那麼，在那個運用工作上，受託運用者就會被視為控管者，且可能因為超出控管者的指示而受到裁罰。

Relationship between controller and processor
控管者與受託運用者的關係

A controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. Elements to be taken into account could be the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism.
控管者委託的受託運用者，必須能夠充分保證將執行適當的技術上與組織上方法，以便其運用活動符合 GDPR 的規定。考量因素可能是受託運用者的專業知識（例如，關於安全措施與個資侵害的技術專業）、受託運用者的可靠程度、受託運用者的資源和受託運用者遵守認可的行為準則或認證機制。

Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on standard contractual clauses.
受託運用者運用個人資料，必須受到契約或有拘束力的其他書面（包含電子形式）法律文件所規範。控管者和受託運用者可以選擇協商他們彼此間的委託合約要包含的所有強制規定，或部分或全部依據標準契約條款。

The GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.
GDPR 列出委託契約應記載事項。然而，委託契約不應只是重述 GDPR 條文，而應該包含更明確和具體的內容，包括如何遵守相關規定以及個人資料運用需要何種安全層級，此即為委託契約之目的。

Relationship among joint controllers
共同控管者間的關係

Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.
共同控管者應以透明方式確定並商定各自責任，以遵守 GDPR 規定的義務。確定各自責任時，必須特別考慮當事人權利的行使和對他們告知的義務。除此之外，責任分配應涵蓋控管者的其他義務，例如，關於一般資料保護原則、法律依據、安全措施、資料外洩通知義務、資料保護影響評估、受託運用者的委託、移轉至第三國，以及與當事人和監管機關之聯繫。

Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.
每個共同控管者都有責任確保他們有運用資料的法律依據，並且不會以共享資料之控管者原始蒐集目的不相符的方式進一步運用資料。

The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject.
GDPR 未明確規定共同控管者之間安排的法定形式。為了法律明確性起見，且為了透明性和課責性，歐盟個人資料保護委員會(EDPB)建議以具有約束力的文件進行此類安排，例如，依據歐盟或成員國法律簽訂以控管者為當事人的合約或其他具有法律約束力的文件。

The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the essence of the arrangement shall be made available to the data subject.
該安排應適當反映共同控管者相對於當事人的各自角色和彼此關係，並應向當事人說明該安排的要旨。

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.
無論安排的條款如何，當事人可以對個別共同控管者行使權利或對抗之。無論是作為共同控管者的資格問題或指定聯絡點的問題，監管機關不受該安排條款的約束。

Table of contents
目錄

EXECUTIVE SUMMARY 2
摘要 2
INTRODUCTION 11
導言 11
PART I – CONCEPTS 13
第一部　概念 13
1　GENERAL OBSERVATIONS 13
1　一般觀察 13
2　DEFINITION OF CONTROLLER 16
2　控管者的定義 16
2.1 Definition of controller 16
2.1 控管者的定義 16
2.1.1“Natural or legal person, public authority, agency or other body” 17
2.1.1「自然人或法人、公務機關、機構或其他團體」 17
2.1.2“Determines” 19
2.1.2「決定」 19
2.1.3“Alone or jointly with others” 26
2.1.3「單獨或與他人共同」 26
2.1.4“Purposes and means” 26
2.1.4「目的和方式」 26
2.1.5“Of the processing of personal data” 33
2.1.5「運用個人資料」 33
3　DEFINITION OF JOINT CONTROLLERS 36
3　共同控管者的定義 36
3.1 Definition of joint controllers 36
3.1 共同控管者的定義 36
3.2 Existence of joint controllership 37
3.2 共同控管的形成 37
3.2.1General considerations 37
3.2.1一般考量 37
3.2.2Assessment of joint participation 38
3.2.2.　評估共同參與 38
3.2.1.1 Jointly determined purpose(s) 41
3.2.1.1 共同決定目的 41
3.2.1.2 Jointly determined means 43

3.2.1.2 共同決定方式 43
3.2.3Situations where there is no joint controllership 49
3.2.3沒有共同控管的情況 49
4 DEFINITION OF PROCESSOR 52
4 受託運用者的定義 52
5 DEFINITION OF THIRD PARTY/RECIPIENT 60
5. 第三方／接收方的定義 60
PART II – **CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES** 64
第二部—歸因於不同角色的結果 64
1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR 64
1. 控管者與受託運用者的關係 64
1.1 Choice of the processor 65
1.1 選擇受託運用者 65
1.2 Form of the contract or other legal act 67
1.2 合約或其他法律文件的形式 67
1.3 Content of the contract or other legal act 72
1.3 合約或其他法律文件的內容 72
1.3.1The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR) 75
1.3.1 受託運用者應僅運用控管者以書面文件指示的資料（GDPR 28(3)(a)條） 75
1.3.2The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR) 77
1.3.2 受託運用者必須確定獲得授權運用個人資料者已承諾保密或有適當法定保密義務（GDPR 第 28（3）（b）條） 77
1.3.3The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR) 78
1.3.3 受託運用者必須採取依 32 條（GDPR 第 28（3）（c）條）規定的一切方法 78
1.3.4 The processor must respect the conditions referred to in Article 28(2) and 1.3.4 28(4) for engaging another processor (Art. 28(3)(d) GDPR). 80
1.3.5 The processor must assist the controller for the fulfilment of

its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR). 81
1.3.5 受託運用者必須協助控管者履行它的義務以回應當事人行使權利的要求（GDPR 第 28（3）（e）條）..... 81
1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR). 82
1.3.6 受託運用者必須協助控管者確實遵守依第 32 到 36 條（GDPR 第 28（3）（f）條）規定的義務 82
1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR). 85
1.3.7 終止運用活動時，在控管者選擇下，受託運用者必須刪除或把所有個人資料歸還控管者並刪除現有副本（GDPR 第 28（3）（g）條） 85
1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR). 86
1.3.8 受託運用者必須提供控管者所有證明遵守第 28 條規定義務所需的資訊，並允許和協助由控管者或另一名由控管者委任的審計人員進行查核，包括檢查（GDPR 第 28（3）（h）條） 86
1.4 Instructions infringing data protection law 88
1.4 違反資料保護法的指示 88
1.5 Processor determining purposes and means of processing 89
1.5 受託運用者決定運用的目的和方法 89
1.6 Sub-processors 89
1.6 次受託人 89
2 CONSEQUENCES OF JOINT CONTROLLERSHIP 93
2 共同控管的結果 93
2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR 93
2.1 以透明方法確定共同控管者遵守 GDPR 義務的個別責任 93

2.2 Allocation of responsibilities needs to be done by way of an arrangement 98
2.2 責任分配需要透過安排 98
2.2.1 Form of the arrangement 98
2.2.1 安排的形式 98
2.2.2. Obligations towards data subjects 99
2.2.2 對當事人的義務 99
2.3 Obligations towards data protection authorities 103
2.3 對資料保護機關的義務 103
Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice 104
附錄 I–控管者、受託運用者及共同控管者概念之應用流程圖 104

The European Data Protection Board
歐盟個人資料保護委員會

Having regard to Article 70 (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, (hereinafter "GDPR" or "the Regulation"),
依據歐洲議會和歐盟理事會於 2016 年 4 月 27 日通過保護自然人關於個人資料運用*和自由流通的 2016/679/EU 個人資料保護規則第 70(1e)條規定，並廢止 95/46/EC 指令（下稱「GDPR」或「規則」），

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],
依據歐洲經濟區聯合委員會 2018 年 7 月 6 日第 154/2018 號決議修正的歐洲經濟區合約，特別是其附件 11 和第 37 號議定書，

Having regard to Article 12 and Article 22 of its Rules of Procedure,
依據其議事規則第 12 條和第 22 條規定，

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges;
本指引的準備工作，包括透過書面和利害關係人會議蒐集利害關係人的意見，以辨識最迫切的挑戰；

HAS ADOPTED THE FOLLOWING GUIDELINES
通過以下指引

INTRODUCTION
導言

* 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」。

1 References to "Member States" made throughout this document should be understood as references to "EEA Member States".
本文件所稱「會員國」係指「歐洲經濟區會員國」。

1. This document seeks to provide guidance on the concepts of controller and processor based on the GDPR's rules on definitions in Article 4 and the provisions on obligations in chapter IV. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.
本文件旨在依據 GDPR 第 4 條定義和第 4 章義務的規定，就控管者和受託運用者的概念提供指引。主要目的在澄清概念的含義，及相關人等的不同角色和彼此間的責任分配。

2. The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5. Moreover, the GDPR also introduces more specific rules on the use of processor(s) and some of the provisions on personal data processing are addressed - not only to controllers - but also to processors.
控管者的概念及其與受託運用者概念的相互作用在 GDPR 的應用上扮演關鍵角色，因為它們決定誰應為遵守不同的資料保護規定負責，以及實際上，當事人如何行使其權利。GDPR 明確引入課責性，即控管者應對第 5 條中與運用個人資料相關的原則負責並證明能遵守。此外，GDPR 也引入更具體的受託運用者（們）使用規則並提出一些關於個人資料運用的規定—不僅針對控管者，也針對受託運用者。

3. It is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the European Union and the EEA.
因此，至關重要的是，這些概念的確切含義及其正確使用的標準足夠清楚，並在整個歐盟和歐洲經濟區共享。

4. The Article 29 Working Party issued guidance on the concepts of controller/processor in its opinion 1/2010 (WP169)[2] in order to provide clarifications and concrete examples with respect to these concepts. Since the entry into force of the GDPR, many questions have been raised regarding to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles. Questions were raised in particular to the substance and implications of the concept of joint controllership (e.g. as

[2] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010, 264/10/EN, WP 169
第 29 條工作小組第 1/2010 號意見關於「控管者」和「受託運用者」的概念， 2010 年 2 月 16 日通過 264/10/EN 第 WP 169 號指引。

laid down in Article 26 GDPR) and to the specific obligations for processors laid down in Chapter IV (e.g. as laid down in Article 28 GDPR). Therefore, and as the EDPB recognizes that the concrete application of the concepts needs further clarification, the EDPB now deems it necessaryto give more developed and specific guidance in order to ensure a consistent and harmonised approach throughout the EU and the EEA. The present guidelines replace the previous opinion of Working Party 29 on these concepts (WP169).
第 29 條工作小組在其第 1/2010 號意見(WP169)發布關於控管者／受託運用者概念的指引，以提供有關這些概念的說明和具體案例。自 GDPR 生效以來，關於 GDPR 對控管者和受託運用者的概念以及它們各自的角色之變化，人們提出了許多問題。尤其是對共同控管概念的內容和含義（例如，GDPR 第 26 條的規定）以及第 4 章規定的受託運用者明確義務（例如，GDPR 第 28 條的規定）的問題。且由於 EDPB 理解這些概念的具體應用需要進一步澄清，EDPB 現在認為有必要提供更成熟和具體的指引，以確保在整個歐盟和歐洲經濟區採用一致且協調的方法。本指引取代第 29 條工作小組先前關於這些概念的意見（WP169）。

5. In part I, these guidelines discuss the definitions of the different concepts of controller, joint controllers, processor and third party/recipient. In part II, further guidance is provided on the consequences that are attached to the different roles of controller, joint controllers and processor.
本指引第一部分討論控管者、共同控管者、受託運用者和第三方／接收者等不同概念的定義。第二部分就控管者、共同控管者和受託運用者的不同角色所帶來的結果提供進一步指引。

PART I – CONCEPTS
第一部　概念

1 GENERAL OBSERVATIONS
1 一般觀察

6. The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:
- the controller shall be *responsible for the compliance* with the principles set out in Article 5(1) GDPR; and that
- the controller shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.

GDPR 第 5(2)條明確引入課責性，意指：
- 控管者者應遵守 GDPR 第 5(1)條規定的原則；而且
- 控管者應能夠證明遵守 GDPR 第 5(1)條規定的原則。

This principle has been described in an opinion by the Article 29 WP[3] and will not be discussed in detail here.
第 29 條工作小組的意見中已敘述此原則，此處不再詳細討論。

7. The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance.[4]
將課責性納入 GDPR 並使其成為核心原則的目的，在強調資料控管者必須實施適當且有效的措施並能夠證明其能遵守。

8. The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28, which lays down the controller's obligations when engaging a processor.
第 24 條進一步闡述課責性，說明控管者應實施適當的技術上和組織上措施，以確保並能證明運用活動依據 GDPR 之規定。如有必要，應審查和更新這些措施。課責性也反映在第 28 條，該條規定控管者在委任受託運用者時的義務。

9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.
課責性直接針對控管者。但是，一些更具體的規定則針對控管者和受託運用者雙方，例如，第 58 條中關於監管機關權力的規定。如果不遵守 GDPR 中與他們相關的義務，控管者和受託運用者都可能被處以罰款，且雙方都有義務依據要求維護和提供適切文件、在調查時配合並

---

[3] Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173.
第 29 條工作小組關於課責性原則的第 3/2010 號意見，2010 年 7 月 13 日通過 00062/10/EN 第 WP 173 號指引。

[4] Recital 74 GDPR
GDPR 前言第 74 段。

遵守行政命令，並直接對監管機關負責。同時，應該記住，受託運用者必須始終遵守且只能按照控管者的指示行事。

10. The accountability principle, together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility, therefore makes it necessary to define the different roles of several actors involved in a personal data processing activity.
因此，課責性以及關於如何遵守 GDPR 和責任分配的其他更具體規定，使得定義參與個人資料運用活動的數個參與者的不同角色變得有必要。

11. A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same.
一般觀察 GDPR 中控管者和受託運用者概念與指令 95/46/EC 相比，並沒有改變，整體而言，如何劃分不同角色的標準仍然一樣。

12. The concepts of controller and processor are *functional* concepts: they aim to allocate responsibilities according to the actual roles of the parties.[5] This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract).[6] This means that the allocation of the roles usually should stem from an analysis of the factual elements or circumstances of the case and as such is not negotiable.
控管者和受託運用者的概念是功能性概念：它們旨在依據各方的實際角色分配責任。這意味行為者，是「控管者」或「受託運用者」的法律地位，原則上必須由其在特定情況下的實際活動來確定，而不是依據行為者被正式指定為「控管者」或「受託運用者」(例如在合約中)。這是指角色的分配通常應源自於對案件事實要素或情況的分析，因此不可協商。

13. The concepts of controller and processor are also *autonomous* concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection

---

5 Article 29 Working Party Opinion 1/2010, WP 169, p. 9.
第 29 條工作小組 1/2010 意見，第 WP 169 號指引，第 9 頁。

6 See also the Opinion of Advocate General Mengozzi, in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:57, paragraph 68 ("*For the purposes of determining the 'controller' within the meaning of Directive 95/46, I am inclined to consider [....] that excessive formalism would make it easy to circumvent the provisions of Directive 95/46 and that, consequently, it is necessary to rely upon a more factual than formal analysis [...].*")
另見法務官 Mengozzi 對耶和華見證人案 C-25/17，ECLI:EU:C:2018:57，第 68 段意見，（「為了確定 95/46 指令所指的「控管者」，我傾向於考慮（……）過度形式主義會使規避 95/46 指令變得容易，因此，有必要依靠依據事實而非形式分析（……）。」）

law. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights or competition law.
控管者和受託運用者的概念在某種意義上也是自主概念，雖然外部法律來源有助識別誰是控管者，但主要應依據歐盟資料保護法來解釋。控管者的概念不應受到法律其他領域的其他（有時相互衝突或重疊的）概念的損害，例如，智慧財產權或競爭法中的創作者或權利人。

14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of 'controller' should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects[7] to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor.
由於賦予控管者角色的基本目標是確保課責性及對個人資料的有效和全面保護，「控管者」的概念應以足夠廣泛的方式解釋，以利盡可能有效且完整保護當事人，以確保歐盟資料保護法的充分效力，避免出現缺漏並防止規避規定的可能，而同時不削弱受託運用者的角色。

2 DEFINITION OF CONTROLLER
2 控管者的定義

2.1 Definition of controller
2.1 控管者的定義

15. A controller is defined by Article 4(7) GDPR as

*"**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**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be **provided for by Union or Member State law**".*
GDPR 第 4(7)條定義控管者為

[7] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, paragraph 34; CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 28; CJEU, Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, judgment of 29 July 2019, paragraph 66.
CJEU，C-131/12 案「Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González」，2014 年 5 月 13 日判決，第 34 段；CJEU，C-210/16 案「Wirtschaftsakademie Schleswig-Holstein」，2018 年 6 月 5 日判決，第 28 段；CJEU，C-40/17 案「Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV」2019 年 7 月 29 日判決，第 66 段。

「單獨或與他人共同決定運用個人資料的目的和方式的自然人或法人、公務機關、機構或其他團體；如果這類運用的目的和方式由歐盟或會員國法律確定，則控管者或其認定的具體標準可由歐盟或會員國法律規定」。

16. The definition of controller contains five main building blocks, which will be analysed separately for the purposes of these Guidelines. They are the following:
控管者的定義包含五個主要組成部分，為本指引之目的分別加以分析，分別是：
    - "the natural or legal person, public authority, agency or other body"
      「自然人或法人、公務機關、機構或其他團體」
    - "determines"
      「決定」
    - "alone or jointly with others"
      「單獨或與他人共同」
    - "the purposes and means"
      「目的和方式」
    - "of the processing of personal data".
      「個人資料的運用」

2.1.1 "Natural or legal person, public authority, agency or other body"
2.1.1 「自然人或法人、公務機關、機構或其他團體」

17. The first building block relates to the type of entity that can be a controller. Under the GDPR, a controller can be "*a natural or legal person, public authority, agency or other body*". This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.[8] In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment acts as a controller or processor, e.g. when processing data on behalf of the parent company.

[8] For example, in its Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75, the CJEU considered that a religious community of Jehovah's witnesses acted as a controller, jointly with its individual members. Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
例如，在耶和華見證人的判決 C-25/17, ECLI:EU:C:2018:551 第 75 段中，CJEU 考量耶和華見證人的宗教社群及其個別成員共同擔任控管者。耶和華見證人的判決 C-25/17, ECLI:EU:C:2018:551 第 75 段。

第一個組成部分與可以成為控管者的實體類型有關。依據GDPR規定，控管者可以是「自然人或法人、公務機關、機構或其他團體」。這意指，原則上，可以擔任控管者角色的實體類型沒有限制。它可能是一個組織，但也可能是一個人或一群人。但實際上，通常是組織本身，而不是組織內的個人（例如，執行長、員工或董事會成員）擔任 GDPR 含義的控管者。就公司集團內的資料運用而言，必須特別注意企業是否擔任控管者或受託運用者的問題，例如，代表母公司運用資料時。

18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing operations. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller.
有時，公司和公共機構會指定特定人員負責執行資料運用。即使指定特定的自然人以確保遵守資料保護規定，這個人也不會是控管者，而是代表法人實體（公司或公共機構）行事，如有違反規定的情況，法人實體將以控管者的身分承擔最終責任。

Example:
案例：

The marketing department of Company ABC launches an advertising campaign to promote ABC's products. The marketing department decides the nature of campaign, the means to be used (e-mail, social media ...), which customers to target and what data to use in order to make the campaign as successful as possible. Even if the marketing department acted with considerable independence, Company ABC will in principle be considered as the controller seeing as the advertising campaign is launched by the company and takes place within the realm of its business activities and for its purposes.
ABC 公司的行銷部門發布廣告宣傳 ABC 的產品。行銷部門決定活動性質、使用方式（電子郵件、社群媒體.....）、目標客群以及使用哪些資料，以使活動盡可能成功。即使行銷部門的運作相當獨立，原則上，ABC 公司仍將被視為控管者，因為廣告活動是由公司發起並在其業務活動範圍內為其目的而進行。

19. In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation's control.[9] In exceptional circumstances,

[9] Employees who have access to personal data within an organisation are generally not considered as "controllers" or "processors", but rather as "persons acting under the authority of the controller or of the processor" within the meaning of article 29 GDPR.

however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar). It is therefore the organisation's duty as controller to make sure that there are adequate technical and organizational measures, including e.g. training and information to employees, to ensure compliance with the GDPR.[10]
原則上，員工在組織的活動範圍內進行的任何個人資料運用都可以推定是在該組織的控管下進行。然而，在例外情況時，可能會發生員工決定將個人資料用於自己的目的，因此超過其被授予的權限而違法。（例如，成立自己的公司或類似情況）。因此，組織作為控管者，有責任確保有足夠的技術上和組織上措施，包括，例如，提供員工訓練和資料，以確保遵守 GDPR 規定。

2.1.2 "Determines"
2.1.2 「決定」

20. The second building block of the controller concept refers to the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*. A controller is a body that *decides* certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. One should look at the specific processing operations in question and understand who determines them, by first considering the following questions: "*why is this processing taking place*?" and "*who decided that the processing should take place for a particular purpose?"*.
控管者概念的第二個組成部分是指控管者藉由行使決策權對運用產生影響。控管者是決定運用過程某些關鍵元素的人。這種控制權可能由法律定義，也可能源於對案件的事實要素或情況的分析。人們應該細查正在討論的特定運用工作，並首先考慮以下問題：「為什麼要運用？」以及「誰決定應該為特定目的進行運用？」以瞭解是誰的決定。

Circumstances giving rise to control
引起控管的情況

21. Having said that the concept of controller is a functional concept, it is therefore based on a **factual rather than a formal analysis**. In order to facilitate the analysis, certain rules of thumb and practical presumptions may be used to guide and simplify the process. In most situations, the

在組織中存取個人資料的員工，通常不被視為「控管者」或「受託運用者」，而是依 GDPR 第 29 條定義為「在控管者或受託運用者權限下行事的人」。

[10] Article 24(1) GDPR.
GDPR 前言第 24(1)條。

"determining body" can be easily and clearly identified by reference to certain legal and/or factual circumstances from which "influence" normally can be inferred, unless other elements indicate the contrary. Two categories of situations can be distinguished: (1) control stemming from *legal provisions*; and (2) control stemming from *factual influence*.
既然說控管者的概念是一個功能性的概念，其是基於事實而非形式的分析。為了方便分析，可以使用某些經驗法則和實際假設來指導和簡化該過程。在大多數情況下，「決定機構」可以很容易且清楚地透過參照某些法律和／或事實情況而確定，從這些情況中通常可以推斷出有「影響」，除非其他要素顯示相反情況。可以區分出有二類情況：(1)源於法律規定的控管；(2)來自事實影響的控管。

1) *Control stemming from legal provisions*
源於法律條文的控管

22. There are cases where control can be inferred from explicit legal competence e.g., when the controller or the specific criteria for its nomination are designated by national or Union law. Indeed, Article 4(7) states that "*where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*" While Article 4(7) only refers to "the controller" in the singular form, the EDPB considers that it may also be possible for Union or Member State law to designate more than one controller, possibly even as joint controllers.
在某些情況下，可以從明確的法律權限中推斷出控管權，例如，當控管者或其認定的具體標準由國家或歐盟法律指定時。事實上，第 4(7)條規定，「如果此類運用的目的和方式由歐盟或會員國法律決定，則控管者或其認定的具體標準可由歐盟或會員國法律規定之。」雖然第 4(7)條僅以單數形式提及「控管者」，但 EDPB 認為，歐盟或成員國法律也可以指定多個控管者，甚至可能成為共同控管者。

23. Where the controller has been specifically identified by law this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control. In some countries, the national law provides that public authorities are responsible for processing of personal data within the context of their duties.
在法律明確確定控管者時，這將決定誰擔任控管者。這預設立法者已將真正有能力行使控管權的實體指定為控管者。在有些國家，國家法律規定公務機關負責在其職責範圍內運用個人資料。

24. However, more commonly, rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, sets up a database or register in order to fulfil those public tasks. In that case, the law, albeit indirectly, sets out who is the controller. More generally, the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as controllers with respect to the processing that is necessary to execute this obligation.
然而，更常見的是，法律會規定一項任務或賦予某人蒐集和運用某些資料的義務，而不是直接任命控管者或規定任命標準。在那些情況裡，運用的目的通常由法律決定。控管者通常是由法律指定以實現此目的、此公共任務的人。例如，當一個實體受委託執行某些公共任務（例如，社會安全），且若不蒐集一些個人資料，建立或登錄個人資料庫就無法完成那些公共任務。那種情況，雖然間接，但法律說明了誰是控管者。更常見的是，法律還可能加諸公共或私人實體保留或提供某些資料的義務。這些實體，就執行此義務所必須的運用而言，通常會被視為控管者。

Example: Legal provisions
案例：法律規定

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.
A 國的國家法律規定，市政當局有義務依據市民的財務狀況提供社會福利，例如，每月補助金。為了付款，市政當局必須蒐集和運用有關申請人財務狀況的資料。儘管，法律沒有明確說明市政當局是此運用的控管者，但這隱含在法律條文中。

2) *Control stemming from factual influence*
源於事實影響的控管

25. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question.
於控管欠缺相關法律規定，擔任控管者之一方，其資格必須以對運用有關的事實評估為準。必須考慮所有相關的事實，以推斷特定實體是否對所討論的個人資料運用產生決定性影響。

26. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.
評估事實的需要也表示，控管者的角色並非源於運用資料的實體本質，而是源於它在特定背景下的具體活動。換句話說，同一個實體可能同時是某些運用的控管者和其他運用的受託運用者，而控管者或受託運用者的資格必須就每個特定的資料運用活動評估而判斷。

27. In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view. This can be due to more general legal provisions or an established legal practice in different areas (civil law, commercial law, labour law etc.). In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, for example an employer in relation to processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors. When an entity engages in processing of personal data as part of its interactions with its own employees, customers or members, it will generally be the one who factually can determine the purpose and means around the processing and is therefore acting as a controller within the meaning of the GDPR.
實際上，從資料保護的角度來看，某些運用活動可被視為與最終承擔責任的實體角色或活動自然相連。這可能是由於較普遍的法律規定或不同領域（民法、商法、勞動法等）的既定法律慣例。在這種情況下，通常包含某種責任的現存傳統角色和專業知識將有助於識別控管者，例如雇主運用其僱員的個人資料、出版商運用其訂戶的個人資料，或協會運用其會員或捐款人的個人資料。當一個實體在與自己的員工、

客戶或會員互動的過程中運用個人資料時，它通常是實際上能決定運用的目的和方式的人，因此為 GDPR 含義上的控管者。

Example: Law firms
案例：法律事務所

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.
ABC 公司聘請一家法律事務所在一件糾紛中擔任代理人。為了執行這項任務，法律事務所需要運用與案件有關的個人資料。運用個人資料的原因是法律事務所受委任在法庭上代表客戶。然而，這項委任並非專門針對個人資料運用。法律事務所的行動具有很高的獨立性，例如，決定使用哪些資料以及如何使用這些資料，而且客戶公司並未就個人資料運用給予任何指示。因此，法律事務所為完成作為公司代理人的任務而進行的運用與法律事務所的功能角色相關聯，因此，它被視為該運用的控管者。

Example: Telecom operators[11]:
案例：電信業者

Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from

[11] The EDPB considers that this example, previously included in Recital (47) of Directive 95/46/EC, remains relevant also under the GDPR.
EDPB 認為這個先前包含在指令 95/46/EC 前言第(47)段的案例，在 GDPR 下也有關連。

whom the message originates, rather than the service provider offering the transmission service.
提供諸如電子郵件服務的電子通信服務涉及個人資料的運用。此類服務的提供商通常會被視為經營這類服務所必需的個人資料運用（例如，流量和計費資料）的控管者。如果，提供商的唯一目的和角色是使電子郵件訊息能傳輸，則提供商將不會被視為訊息本身包含的個人資料的控管者。訊息中包含的任何個人資料之控管者通常被認為發出訊息的人，而不是提供傳輸服務的服務提供商。

28. In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as controller. Even if a contract is silent as to who is the controller, it may contain sufficient elements to infer who exercises a decision-making role with respect to the purposes and means of the processing. It may also be that the contract contains an explicit statement as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract. However, the terms of a contract are not decisive in all circumstances, as this would simply allow parties to allocate responsibility as they see fit. It is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else.
在很多情況裡，評估參與的各方之間的合約條款有助於確定哪一方（或多方）擔任控管者。即使，合約沒有說明誰是控管者，它也可能包含足以推斷誰在運用的目的和方式上發揮決策作用的元素。合約也可能包含關於控管者身分的明確說明。如果，沒有理由懷疑這精準反映出事實，那就沒理由反對遵守合約條款。然而，合約條款並非在所有情況下都具有決定性，因為這只是讓各方按照他們認為合適的方式分配責任。不可能僅僅藉由把合約打造成某種樣式，而事實卻顯示其他情況，就成為控管者或逃避控管者的義務。

29. If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor. Similarly, it is not because a commercial contract uses the term "subcontractor" that an entity shall be considered a processor from the perspective of data protection law.[12]

[12] See e.g., Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128, p. 11.
參見第 29 條工作小組關於環球銀行金融電信協會（SWIFT）個人資料運用的 10/2006 意見。2006 年 11 月 22 日，第 WP128 號指引，第 11 頁。

如果，一方事實上決定了運用個人資料的原因和方式，即使合約說它是受託運用者，該方也會是控管者。同樣地，從資料保護法的角度來看，並不會因為商業合約使用「分包商」一詞，一個實體就應被視為受託運用者。

30. In line with the factual approach, the word "determines" means that the entity that actually exerts influence on the purposes and means of the processing is the controller. Normally, a processor agreement establishes who the determining party (controller) and the instructed party (processor) are. Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and to be able to request changes if necessary. Furthermore, the processor cannot at a later stage change the essential elements of the processing without the approval of the controller.
依據真實作法，「決定」一詞表示實際影響運用的目的和方式的實體就是控管者。通常，受託運用者合約會確定誰是決定方（控管者）和受指示方（受託運用者）。即使，受託運用者提供一開始就明確定義的服務，控管者也必須獲得服務的詳細描述，並且必須做出主動同意運用的執行方式，並能在必要時要求更改的最終決定。此外，未經控管者同意，受託運用者不能在後續階段更改運用的主要內容。

Example: standarised cloud storage service
案例：標準化雲端儲存服務

A large cloud storage provider offers its customers the ability to store large volumes of personal data. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a "take it or leave it basis". Company X decides to make use of the cloud provider to store personal data concerning its customers. Company X will still be considered a controller, given its decision to make use of this particular cloud service provider in order to process personal data for its purposes. Insofar as the cloud service provider does not process the personal data for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as a processor.
大型雲端儲存提供商提供客戶儲存大量個人資料的能力。該服務完全標準化，客戶幾乎沒有或沒有能力客製化服務。合約條款由雲端服務提供商單方面確定和草擬，以「不接受就拉倒」的方式提供給客戶。X 公司決定使用雲端提供商儲存有關其客戶的個人資料。考量到它

決定使用這個特定的雲端服務提供商，為其目的運用個人資料，X 公司仍將被視為控管者。只要雲端服務提供商不為自己的目的運用個人資料並且僅代表客戶並按其指示儲存資料，則服務提供商將被視為受託運用者。

2.1.3 "Alone or jointly with others"
2.1.3 「單獨或與他人共同」

31. Article 4(7) recognizes that the "purposes and means" of the processing might be determined by more than one actor. It states that the controller is the actor who "alone or jointly with others" determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them then being subject to the applicable data protection provisions. Correspondingly, an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms, as clarified later on.[13]
第 4(7)條察覺，運用的「目的和方式」可能由不止一個行為者決定。它指出，控管者是「單獨或與他人共同」決定運用目的和方式的行為者。這表示數個不同的實體可以擔任同一個運用的控管者，於是每個實體都受適用的資料保護條文約束。因此，即使一個組織沒有就目的和方式做出所有決定，它仍然可以成為控管者。共同控管的標準以及二個或多個參與者共同行使控管的範圍可能有不同形式，後面將予以說明。

2.1.4 "Purposes and means"
2.1.4 「目的和方式」

32. The fourth building block of the controller definition refers to the object of the controller's influence, namely the "purposes and means" of the processing. It represents the substantive part of the controller concept: what a party should determine in order to qualify as controller.
控管者定義的第四個組成部分是指控管者影響的對象，即運用的「目的和方式」。它代表控管者概念的實質部分：一方應決定什麼才夠資格成為控管者。

33. Dictionaries define "purpose" as "an anticipated outcome that is intended or that guides your planned actions" and "means" as "how a result is obtained or an end is achieved".

[13] See section 3, p.15
見第三節第 15 頁。

字典將「目的」定義為「預期的或指引你所規劃行動的結果」，而「方式」定義為「如何獲得結果或達到目的」。

34. The GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the "purposes" of the processing and the "means" to achieve them is therefore particularly important.
GDPR 規定，資料必須為特定、明確和合法目的而蒐集，且不得以與這些目的不相符的方式進行進一步運用。因此，決定運用的「目的」和達成它們的「方式」尤為重要。

35. Determining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing:[14] given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., "to what end"; or "what for") and *how* this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.[15]
決定目的和方式相當於分別決定「為什麼」和「如何」運用：收到特定的運用工作後，控管者是決定為什麼要運用（即「什麼目的」；或「為了什麼」）以及如何達到這一目的（即應採用何種方式達成目標）的行為者。對個人資料的運用行使此類影響的自然人或法人，因而依據 GDPR 第 4(7)條的定義參與決定該運用的目的和方式。

36. The controller must decide on both purpose and means of the processing as described below. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing. Conversely, the party acting as processor can never determine the purpose of the processing.
控管者必須決定如下所述的運用目的和方式。因此，控管者不能只確定目的。它還必須決定運用的方式。反過來說，作為受託運用者的一方永遠無法決定運用的目的。

37. In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB

---

[14] See also the Opinion of Advocate General Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, paragraph 46.
另見法務官 Bot 對「*Wirtschaftsakademie*」案的意見書，C-210/16, ECLI:EU:C:2017:796, 46 段。

[15] Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 68.
「耶和華見證人」案判決，C-25/17, ECLI:EU:C:2018:551，68 段。

recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which **level of influence** on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.
實際上，如果控管者聘請受託運用者代表它進行運用，通常表示受託運用者應能就如何執行運用自行作出某些決定。EDPB 意識到，受託運用者可以有一些操作空間，讓它也能作出一些與運用相關的決定。從這個角度來看，有必要就一個實體擔任控管者的資格對「為什麼」和「如何」發揮何種程度的影響，以及受託運用者可以自行作出決定的範圍有多大提供指引。

38. When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller.
當一個實體清楚決定了目的和方式，以相當於執行其詳細指令的方式委託另一個實體運用時，情況就很明確了，第二個實體無疑應被視為受託運用者，而第一個實體則是控管者。

Essential vs. non-essential means
必要 vs 非必要方式

39. The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make.
問題是保留給控管者的決定與可由受託運用者自行作出的決定該如何界定。關於運用目的的決定顯然是出自控管者。

40. As regards the determination of means, a distinction can be made between essential and non-essential means. “Essential means” are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data which are processed (“*which data shall be processed*?”), the duration of the processing (“*for how long shall they be processed?*”), the categories of recipients (“*who shall have access to them?*”) and the categories of data subjects (“*whose personal data are being processed?*”). “Nonessential means” concern more practical aspects of implementation, such as the choice for a particular type of hard- or software

or the detailed security measures which may be left to the processor to decide on.
關於方式的確定，可以區分為必要方式和非必要方式。「必要方式」與運用的目的和範圍密切相關，傳統上自然應屬控管者。必要方式的案例是運用的個人資料類型(「應運用哪些資料？」)、運用的時間(「運用要多久時間？」)、接收者的類別(「誰可以存取它們？」)和當事人的類別(「正在運用誰的個人資料？」)。「非必要方式」涉及更實際的執行面，例如，選擇特定的硬體或軟體種類，或可能留給受託運用者決定的詳細安全措施。

Example: Payroll administration
案例：薪資管理

Employer A hires another company to administer the payment of salaries to its employees. Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out for Company A's purpose to pay salaries to its employees and the payroll administrator may not use the data for any purpose of its own. The way in which the payroll administrator should carry out the processing is in essence clearly and tightly defined. Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter its role as processor as long as the administrator does not go against or beyond the instructions given by Company A.
雇主 A 聘請另一家公司管理其僱員的薪資發放。雇主 A 明確說明付款對象、金額、日期、銀行、資料應儲存多久、應向稅務機關揭露哪些資料等。在這個案例裡，資料運用是為了 A 公司向其僱員支付薪資的目的而執行,而薪資管理人不得為了任何自己的目的而使用這些資料。基本上，薪資管理人執行運用的方式既明確又經嚴格定義。儘管如此，薪資管理人可以決定有關運用的某些詳細事項，例如，使用哪種軟體，如何在自己的組織內分配存取權限等。這不會改變它擔任受託運用者的角色，只要管理人不違背或超出 A 公司的指示。

Example: Bank payments
案例：銀行付款

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose

of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B's processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.
作為雇主 A 指示的一部分，薪資管理部門將資料傳給 B 銀行，以便他們可以實際支付給雇主 A 的員工。這個工作包括 B 銀行為執行銀行業務而進行的個人資料運用。在這個行動中，銀行為提供這項服務自行決定必須運用哪些資料，資料必須儲存多久等，與雇主 A 無關。雇主 A 對銀行 B 運用資料的目的和方式無法有任何影響。因此，銀行 B 應被視為此運用的控管者，而薪資管理部門傳送個人資料應被視為兩個控管者之間的資訊揭露，即從雇主 A 到銀行 B。

Example: Accountants
案例：會計

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A. Accounting firm C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the data it collects will only be processed for the purpose of auditing A and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use. Under these circumstances, Accounting firm C is to be regarded as a controller of its own when performing its auditing services for A. However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.
雇主 A 還聘請 C 會計師事務所查核帳目，因此將有關財務交易的資料（包括個人資料）傳給 C。C 會計師事務所在沒有 A 的詳細指示下運用這些資料。C 會計師事務所依據規範 C 進行查核工作的法律規定，自行決定它蒐集的資料，只為了查核 A 的目的而加以運用，它決

定它需要有哪些資料，哪些類別的人員需要登錄，資料應保存多久以及使用何種技術工具。在這些情況下，C 會計師事務所在為 A 提供查核服務時，應被視為自己的控管者。但是，依據 A 的指示程度，這種評斷可能會有所不同。在法律沒有規定會計師事務所的明確義務，且客戶公司提供了非常詳細的運用說明時，會計師事務所確實是擔任受託運用者。可以區分成以下情況：依據規範該行業的法律，進行運用是作為會計師事務所核心活動的一部分，以及運用是客戶公司活動的一部分所進行的較有限的輔助任務。

Example: Hosting services
案例：代管服務

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H on, for example, which technical and organisational security measures are required and a data processing agreement according to Article 28 must be concluded. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.
雇主 A 聘請代管服務 H 將加密資料儲存在 H 的伺服器上。代管服務 H 不會確定其代管的資料是否為個人資料，也不會以任何將資料儲存於伺服器以外的方式運用資料。由於儲存是個人資料運用活動的一個案例，而代管服務 H 代表雇主 A 運用個人資料，因此是受託運用者。雇主 A 必須給 H 必要的指示，例如，需要採取哪些技術和組織的安全措施，以及必須包含依據第 28 條而定的資料運用合約。H 必須協助 A 確保採取必要的安全措施，並在任何個人資料外洩時通知它。

41. Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of

natural persons. For this reason, the controller must be fully informed about the means that are used so that it can take an informed decision in this regard. In order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract or other legally binding instrument between the controller and the processor.
即使非必要方式的決定可以留給受託運用者，控管者仍必須在受託運用者合約中訂定某些要素，例如與安全有關之要求，如依據 GDPR 第 32 條採取所有必要措施的指示。合約還必須說明受託運用者應協助控管者確保遵守，例如第 32 條規定。無論如何，控管者仍負責實施適當的技術和組織措施，以確保並能夠證明運用是依據該規則執行（第 24 條）。在此過程中，控管者必須考慮運用的性質、範圍、背景和目的以及自然人的權利與自由之風險。因此，控管者必須充分了解使用的方法，以便在這方面做出有依據的決定。為了使控管者能證明運用的合法性，建議控管者和受託運用者之間的合約或其他具有法律約束力的文書中記錄最低限度的必要技術和組織措施。

Example: Call centre
案例：電話客服中心

Company X decides to outsource a part of its customer service relations to a call centre. The call centre receives identifiable data about customer purchases, as well contact information. The call centre uses its own software and IT infrastructure to manage the personal data concerning Company X's customers. Company X signs a processor agreement with the provider of the call centre in accordance with Article 28 GDPR, after determining that the technical and organisational security measures proposed by the call centre are appropriate for the risks concerned and that the call centre will only process the personal data for the purposes of Company X and in accordance with its instructions. Company X does not provide any further instructions to the call centre as to specific software to be used nor any detailed instructions regarding the specific security measures to be implemented. In this example, Company X remains a controller, despite the fact that the call centre has determined certain non-essential means of the processing.
X 公司決定將部分客戶服務相關業務外包給一家電話客服中心。該電話客服中心收到可資識別的客戶購買資料還有聯絡資料。電話客服中心使用它自己的軟體和 IT 基礎架構管理關於 X 公司客戶的個人資料。X 公司在判定電話客服中心提案的技術和組織安全措施，認為相關風險已足夠，且電話客服中心只會為 X 公司的目的並依其指示運用個人資料後，依據 GDPR 第 28 條，和電話客服中心提供商簽訂

受託運用者合約。X 公司並未給電話客服中心更多指示，如使用特定軟體，或任何關於執行特定安全措施的詳細指示。在這個案例中，X 公司仍是控管者，儘管電話客服中心決定某些運用的非必要方法。

2.1.5 "Of the processing of personal data"
2.1.5 「運用個人資料」

42. The purposes and means determined by the controller must relate to the "processing of personal data". Article 4(2) GDPR defines the processing of personal data as "*any operation or set of operations which is performed on personal data or on sets of personal data*". As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.[16]
控管者決定的目的和方式必須與「個人資料的運用」相關。GDPR 第 4(2)條將個人資料運用定義為「對個人資料或個人資料集執行的任何操作或一系列操作」。因此，控管者的概念可以與單一運用操作或一系列操作相連結。實際上，這可能表示，由特定實體實施的控管可能會擴展到整個運用過程，但也可能僅限於運用過程中的特定階段。

43. In practice, the processing of personal data involving several actors may be divided into several smaller processing operations for which each actor could be considered to determine the purpose and means individually. On the other hand, a sequence or set of processing operations involving several actors may also take place for the same purpose(s), in which case it is possible that the processing involves one or more joint controllers. In other words, it is possible that at "micro-level" the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at "macro-level" these processing operations should not be considered as a "set of operations" pursuing a joint purpose using jointly defined means.

---

[16] Judgment in *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74: "*(A)s the Advocate General noted, [...-] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, [...] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means".*
「Fashion ID」案判決，C-40/17, ECLI:EU:C:2019:629，74 段：「如法務官所指……，看來似乎在 95/46 指令第 2(d)條含義中，自然人或法人如果與他人共同決定個人資料運用目的與方式，可為控管者。相反地，在整個資料運用過程之前或之後不能決定目的與方式的自然人或法人，依據該條規定，不能被視為控管者。」

實際上，涉及多個行為者的個人資料運用可以被劃分為幾個較小的運用操作，可以考慮每個行為者單獨確定目的和方式。另一方面，涉及多個行為者的一系列或一組運用操作也可能出於相同目的而發生，在這種情況下，運用可能涉及一個或多個共同控管者。換句話說，在「微觀層面」，該系列的不同運用操作可能看起來不連貫，因為每一個都可能有不同目的。但是，必需再次檢查這些運用操作是否在「宏觀層面」不應被視為使用共同定義的方式追求共同目的的「一組操作」。

44. Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a "controller" even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.
任何決定運用資料的人都必須考慮這是否包括個人資料，如果是，依據 GDPR 規定的義務是什麼。即使行為者沒有像這樣蓄意針對個人資料或錯誤地評斷它沒有運用個人資料，行為人也將被視為「控管者」。

45. It is not necessary that the controller actually has access to the data that is being processed.[17] Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.
控管者實際上未必會存取正在運用的資料。將運用活動外包並在此過程中對運用目的和（必要）方式具有決定性影響（例如，透過調整服務參數而對運用誰的個人資料有影響）的人就被視為控管者，即使他們從未真正存取資料。

Example: Market research 1
案例：市場研究 1

Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.
ABC 公司希望了解哪些類型的消費者最有可能對其產品感興趣，與服務提供商 XYZ 簽訂合約以獲得相關資料。

[17] Judgment in *Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI :EU :C :2018 :388, paragraph 38.
「*Wirtschaftsakademie Schleswig-Holstein GmbH*」*案判決*, C-201/16，ECLI :EU :C :2018 :388，第 38 段。

Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research.
ABC 公司向 XYZ 說明它對什麼類型的資料感興趣，並提供一份要向參與市場研究的人提出的問題清單。

Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.
ABC 公司僅從 XYZ 接收統計資料（例如，確定每個地區的消費者趨勢），並未存取個人資料。然而，ABC 公司決定應進行運用，運用是為了它的目的和活動而進行，且它已提供 XYZ 關於蒐集哪些資料的詳細指示。因此，就執行個人資料運用以傳送它要求的資料而言，ABC 公司仍應被視為控管者。XYZ 只能因為 ABC 公司給的目的並依據其詳細指示運用資料，因此被視為受託運用者。

Example: Market research 2
案例：市場研究 2

Company ABC wishes to understand which types of consumers are most likely to be interested in its products. Service provider XYZ is a market research agency which has collected information about consumer interests through a variety of questionnaires which pertain to a wide variety of products and services. Service provider XYZ has collected and analysed this data independently, according to its own methodology without receiving any instructions from Company ABC. To answer Company ABC's request, service provider XYZ will generate statistical information, but does so without receiving any further instructions about which personal data should be processed or how to process it in order to generate these statistics. In this example, service provider XYZ acts as the sole controller, processing personal data for market research purposes, autonomously determining the means for doing so. Company ABC does not have any particular role or responsibility under data protection law in relation to these processing activities, as Company ABC receives anonymised

statistics and is not involved in determining the purposes and means of the processing.
ABC 公司想瞭解哪種類型的消費者對公司產品比較感興趣。XYZ 提供市場研究服務，透過廣泛的各式產品與服務問卷，蒐集有關消費者感興趣的資料。XYZ 未經 ABC 公司指示，即已根據本身的方法論，獨立蒐集和分析了這些資料。為回應 ABC 公司要求，XYZ 將產出統計資料，但不會為此接受進一步指示來決定運用何種個人資料或如何運用個人資料。在這個案例中，服務提供商 XYZ 為市場研究目的而運用個人資料，並自主決定運用方式，為資料的獨立控管者。ABC 公司接收匿名化的統計資料，未介入決定資料運用的目的和方式，因此在資料保護法下，對於這些運用活動不具有任何特別的角色或責任。

3 DEFINITION OF JOINT CONTROLLERS
3 共同控管者的定義

3.1 Definition of joint controllers
3.1 共同控管者的定義

46. The qualification as joint controllers may arise where more than one actor is involved in the processing.
共同控管者的資格可能因運用過程中涉及多個行為者而產生。

47. While the concept is not new and already existed under Directive 95/46/EC, the GDPR, in its Article 26, introduces specific rules for joint controllers and sets a framework to govern their relationship. In addition, the Court of Justice of the European Union (CJEU) in recent rulings has brought clarifications on this concept and its implications[18].
雖然，這並非新概念，且在 95/46/EC 號指令下已存在，但 GDPR 第 26 條制定了共同控管者的具體規定，並設定規範他們關係的框架。此外，歐盟法院（CJEU）在近期裁決中，已闡明這個概念及其含意。

48. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of

[18] See in particular, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C210/16), *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (*C-40/17). To be noted that while these judgments were issued by the CJUE on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.
特別參見 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C210/16), *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (*C-40/17)。請注意，雖然這些判決是 CJUE 為解釋在 95/46/CE 指令的共同控管者概念而作出，在 GDPR 仍然有效，因為 GDPR 與指令決定這個概念的要素。

obligations for compliance with data protection rules and in particular with respect to the rights of individuals.
正如第二部分第 2 節進一步闡述的那樣，共同控管者的資格主要影響遵守資料保護規定的義務分配，特別是個人權利方面。

49. In this perspective, the following section aims to provide guidance on the concept of joint controllers in accordance with the GDPR and the CJEU case law to assist entities in determining where they may be acting as joint controllers and applying the concept in practice.
從這個角度來看，下節旨在依據 GDPR 和 CJEU 判例法就共同控管者的概念提供指引，以幫助實體確定他們可以擔任共同控管者的情況，並將這個概念應用於實務上。

3.2 Existence of joint controllership
3.2 共同控管的形成

3.2.1 General considerations
3.2.1 一般考量

50. The definition of a controller in Article 4 (7) GDPR forms the starting point for determining joint controllership. The considerations in this section are thus directly related to and supplement the considerations in the section on the concept of controller. As a consequence, the assessment of joint controllership should mirror the assessment of "single" control developed above.
GDPR 第 4(7)條對控管者的定義形成確定共同控管的起點。因此，本節中的考量與控管者概念該節中的考量直接相關並加以補充。因此，對共同控管的評定應反映上述對「單一」控管的評估。

51. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that *"[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."* In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine *jointly* the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.
GDPR 第 26 條反映了 GDPR 第 4(7)條的定義，規定「在二個或多個控管者共同決定運用的目的和方式時，他們應為共同控管者。」廣義而言，在特定運用活動上，由不同的人共同決定該運用活動的目的和方式，就形成共同控管。因此，評定共同控管者的存在需要檢查控管者特

有的目的和方式的決定是否不止由一方為之。「共同」必須依不同的形式和組合解釋為「一起」或「不單獨」，如下所述。

52. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.
對共同控管的評定應基於對運用目的和方式之實際影響的事實分析，而不是形式分析。所有現有或預想的安排都應依據雙方關係的實際情況進行核對。只有形式上的標準是不夠的，理由至少有二個：在某些情況下，沒有共同控管者的正式任命（例如，法律或合約規定）；而在其他情況，正式任命可能未反映真正的安排，而是將控管者的角色正式委託給實際上無法「決定」運用目的和方式的實體。

53. Not all processing operations involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the **joint participation of two or more entities in the determination of the purposes and means** of a processing operation. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.
並非所有涉及多個實體的運用操作都會產生共同控管。存在共同控管的首要標準是二個或多個實體共同參與決定運用操作的目的和方式。更具體地說，共同參與需要一方面包括目的的確定，另一方面包括方式的確定。如果，這些要素每一個都由所有相關實體決定，則它們應被視為此討論的運用的共同控管者。

3.2.2 Assessment of joint participation
3.2.2. 評估共同參與

54. Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a

common decision taken by two or more entities or result from **converging decisions** by two or more entities regarding the purposes and essential means.
共同參與決定目的和方法意指不止一個實體對是否運用以及如何進行具有決定性影響。實際上，共同參與可以有數種不同形式。例如，共同參與可以是二個或以上的實體共同決定，也可以是二個或以上的實體就目的和必要方式一致決定的結果。

55. Joint participation through a *common decision* means deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.
透過共同決定來共同參與是指一起決定，且包含符合 GDPR 第 26 條所指「共同」一詞最普遍認知的共同意向。
The situation of joint participation through *converging decisions* results more particularly from the case law of the CJEU on the concept of joint controllers. Decisions can be considered as converging on purposes and means **if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing**. It should be highlighted that the notion of converging decisions needs to be considered in relation to the purposes and means of the processing but not other aspects of the commercial relationship between the parties.[19] As such, an important criterion to identify converging decisions in this context **is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.** The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller.
透過一致決定共同參與的情況，更確切地說，是由於歐盟法院關於共同控管者概念的判例法而產生。如果這些決定彼此互補且是以對於決定運用的目的和方式有實質影響的方式進行運用之所需，則決定可被視為在目的和方式上一致。應該強調的是，共同決定的概念需要考慮的是運用的目的和方式，而不是當事人間商業關係的其他方面。因此，在這種情況下識別一致決定的一個重要標準是，如果沒有雙方的參與，是否不可能運用，因為每一方的運用是不可分割的，亦即緊密連結。然而，共同控管者基於一致決定而行事的情況應與受託運用者的情況有

[19] Indeed, all commercial arrangements involve converging decisions as part of the process by which an agreement is reached.
事實上，所有商業安排都包含達成合約過程一部分的共同決定。

所區別，因為後者在參與運用的執行時，不會為了自己的目的而運用資料，而是代表控管者進行運用。

56. The fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership[20]. For example, in *Jehovah's Witnesses*, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.[21] The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing.[22] The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community.[23] In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.[24]
事實上，其中一方無權存取已運用的個人資料並不足以排除共同控管。例如，在「耶和華見證人」案中，歐盟法院認為，必須將宗教團體與其從事傳道的成員，在後者挨家挨戶傳道時運用個人資料的情況中，一起視為控管者。歐盟法院認為該團體不一定要存取提及的資料，或確定該團體已提供其成員與資料運用有關的書面指引或指示。該團體透過組織和協調其成員的活動參與了目的和方式的決定，這有助於實現耶和華見證人的目標。此外，該團體普遍了解進行此類運用是為了傳播其信仰。

57. It is also important to underline, as clarified by the CJEU, that an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the processing. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of

---

20 Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 38.
「Wirtschaftsakademie」案判決，C-210/16, ECLI:EU:C:2018:388，第 38 段。

21 Judgment in Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
「耶和華見證人」案判決，C-25/17, ECLI:EU:C:2018:551，第 75 段。

22 Ibid.
同上。

23 Ibid, paragraph 71.
同上，第 71 段。

24 Ibid.
同上。

processing, this entity must be considered as the sole controller of this preceding or subsequent operation[25].
同樣重要的是要強調，正如歐盟法院所闡明，一個實體僅在其與其他人共同決定運用方式和目的的那些操作活動中，才會與其他人一起被視為共同控管者。如果，這些實體之一單獨決定在運用過程之前或之後的操作目的和方式，則該實體必須被視為該之前或後續操作的唯一控管者。

58. The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, the CJEU has clarified that those operators may be involved at different stages of that processing and to different degrees so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.
共同責任未必指參與運用個人資料的不同操作者責任相同。相反地，歐盟法院已闡明，那些操作者可能參與該運用過程的不同階段且參與程度不同，因此必須依據該特定案件的所有相關情況評估他們每個人的責任。

3.2.1.1 Jointly determined purpose(s)
3.2.1.1 共同決定目的

59. Joint controllership exists when entities involved in the same processing operation process such data for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.
當參與同一運用操作的實體為共同定義的目的而運用此類資料時，就形成共同控管。如果，參與的實體出於相同或共同目的運用資料，就會出現這種情況。

60. In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. In *Fashion ID*, for example,

---

[25] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 74 "*By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*".
「Fashion ID」案判決，C-40/17, ECLI:EU:2018:1039，第 74 段。「相反地，在整個資料運用過程之前或之後不能決定目的與方式的自然人或法人，依據該條規定，不能被視為控管者。」。

the CJEU clarified that a website operator participates in the determination of the purposes (and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed in the economic interests of both the website operator and the provider of the social plug-in.[26]
此外，當實體的運用目的不同時，依據歐盟法院判例法，當參與實體追求密切相關或互補的目的時，也可以確立共同控管。例如，當同一運用操作產生互利時，可能就是這種情況，而每個實體都參與決定相關運用操作的目的和方式。例如，在「Fashion ID」案中，歐盟法院說明，網站經營者透過在網站上嵌入社交外掛程式，讓它的產品在社群網路上的能見度提高而達到最有效的宣傳，參與運用目的（和方式）之決定。歐盟法院認為，此案件的運用操作是為了網站經營者和社交外掛程式提供者的經濟利益而執行。

61. Likewise, as noted by the CJEU in *Wirtschaftsakademie*, the processing of personal data through statistics of visitors to a fan page is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity.[27] Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.[28]
同樣地，正如歐盟法院在「Wirtschaftsakademie」案中所指出，透過粉絲專頁瀏覽者的統計資料運用個人資料，目的在讓 Facebook 能改善透過它的網路傳送的自家廣告系統，並使粉絲專頁的管理員能取得統計資料以管理其活動宣傳。在這種情況下，每個實體都追求自己的利益，但雙方都參與決定運用粉絲專頁瀏覽者個人資料的目的（和方式）。

62. In this respect, it is important to highlight that the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.

---

[26] Judgment in *Fashion ID,* C-40/17, ECLI:EU:2018:1039, paragraph 80.
「Fashion ID」案判決，C-40/17, ECLI:EU:C:2018:1039，第 80 段。

[27] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34.
「Wirtschaftsakademie」案判決，C-210/16, ECLI:EU:C:2018:388，第 34 段。

[28] Judgment in Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, paragraph 39.
「Wirtschaftsakademie」案判決，C-210/16, ECLI:EU:C:2018:388，第 39 段。

在這種情況下，重要的是要強調，僅由運用活動而產生的互利（例如商業）並不會形成共同控管。如果參與運用的實體不追求與運用活動相關的任何自身目的，而只是因提供服務而獲得報酬，則它是受託運用者而不是共同控管者。

3.2.1.2 Jointly determined means
3.2.1.2 共同決定方式

63. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.
共同控管還需要二個或以上的實體影響運用方式。這並不表示，為形成共同控管，每個參與的實體都需要決定所有方式。事實上，正如歐盟法院的說明，不同的實體可能參與不同的運用階段，參與程度也不同。因此，不同的共同控管者可能會在不同程度上定義運用的方式，取決於誰處於實際這樣做的職位。

64. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.
情況也可能是參與的實體之一提供運用方式，並使其他實體可運用個人資料。決定使用這些方式以便為特定目的運用個人資料的實體，也參與運用方式的確定。

65. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up[29]. The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.

[29] The provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor.
如符合上述標準，系統提供者可以是共同控管者，亦即，如果系統提供者參與決定目的和方式。否則，系統提供者應視為受託運用者。

這種狀況會明顯出現在允許各方運用相同個人資料的平台、標準化工具或其他基礎設施，且這些資料是由其中一方以某種方式建立並供其他也可決定如何建立的實體使用。當現有的技術系統用戶可以決定在此情境下執行個人資料運用時，使用該系統並不排除共同控管。

66. As an example of this, the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.
就如歐盟法院在「Wirtschaftsakademie」案中認為，Facebook 上的粉絲專頁管理員，透過依據其目標受眾以及管理和宣傳其活動的目的定義參數，必須被視為參與決定與其粉絲專頁瀏覽者相關的個人資料運用方式。

67. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case where the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing[30].
此外，一個實體選擇為自己的目而使用另一個實體開發以供運用個人資料的工具或其他系統，很可能相當於這些實體對運用方式的共同決定。這是由「Fashion ID」一案而來，歐盟法院在此案的結論是，透過在其網站上嵌入 Facebook 提供給網站經營者的 Facebook 按讚按鈕，Fashion ID 對瀏覽它在 Fackbook 上網站者的個人資料蒐集和傳送的操作產生決定性影響，因此與 Facebook 共同決定該運用的方式。

68. It is important to underline that **the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as** joint **controllers,** in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

[30] Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039, paragraphs 77-79.
「Fashion ID」案判決，C-40/17, ECLI:EU:C:2018:1039，第 77-79 段。

要強調的是，使用普通資料運用系統或基礎設施不會使參與的各方有資格成為共同控管者，尤其是，當他們執行的運用是可分開且可由一方在沒有他方介入下進行，或者提供者是沒有任何自身目的的受託運用者（參與的各方僅有商業利益不足以成為運用的目的）。

Example: Travel agency
案例：旅行社

A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own purposes and there is no joint controllership.
旅行社將客戶的個人資料發送給航空公司和連鎖飯店，以便預訂套裝行程。航空公司和飯店確認所要求的座位和房間可預訂。旅行社發給客戶旅遊證件和票券。每個參與者以其自己之方式運用資料以執行自己的活動。在這種情況下，旅行社、航空公司和飯店是三個不同的資料控管者，為各自的目的運用資料，不存在共同控管。

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internetbased common platform.
旅行社、連鎖飯店和航空公司隨後決定為提供套裝行程的共同目的而共同建立一個網路共用平台。他們就使用的必要方式達成合意，例如將儲存哪些資料、如何分配和確認預訂以及誰可以存取儲存的資料。此外，他們決定共享客戶資料，以便進行聯合行銷活動。在這種情況下，旅行社、航空公司和連鎖飯店共同決定他們各自客戶的個人資料運用目的和方式，因此成為與共用網路預訂平台和聯合行銷活動有關

運用之共同控管者。然而，對於網路共用平台之外的其他運用活動，他們則各自保有單獨的控管權。

Example: Research project by institutes
案例：機構的研究專案

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.
數個研究機構決定參與一個特定的共同研究專案，並為此目的而使用某一參與該專案的機構的現有平台。各研究機構為了共同研究目的，將所持有的個人資料輸入平台，並使用他人透過平台提供的資料進行研究。在這種情況下，所有機構都有資格成為透過儲存和公開來自該平台的資料運用個人資料的共同控管者，因為它們一起決定運用目的和使用的方式（現有平台）。然而，就任何可能出於各自目的在該平台外執行的運用而言，每個機構都是單獨的控管者。

Example: Marketing operation
案例：行銷活動

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions. Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.
A 和 B 公司推出聯名產品 C，希望規劃活動宣傳該產品。為此，他們決定共享來自各自客戶和潛在客戶資料庫的資料，並依此決定活動的受邀名單。他們也談好活動邀請的發送方式、活動期間如何蒐集回饋意見以及後續的行銷活動。A 和 B 公司可被視為與促銷活動規劃相

關的個人資料運用的共同控管者，因為它們共同決定在此情況下的資料運用的目的和必要方式。

Example: Clinical Trials[31]
案例：臨床實驗

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.
醫療照護提供者（調查者）和大學（贊助者）決定共同開展一項具有相同目的的臨床試驗。他們共同合作草擬研究計畫書（亦即研究的目的、方法／設計、要蒐集的資料、受試者排除／納入標準、資料庫重覆使用（如相關）等）。對於本臨床試驗而言，他們可以被視為共同控管者，因為他們共同決定並同意相同的目的和運用的主要方式。為了研究目的從病患的病歷中蒐集個人資料，應與為照護病人的目的儲存和使用相同資料有所區分，醫療照護提供者仍是這方面的控管者。

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.
如果，調查者不參與計畫書的起草（而只是接受贊助者已經制定好的計畫書），且計畫書只由贊助者設計，則應將調查者視為受託運用者，而贊助者為這個臨床試驗的控管者。

Example: Headhunters
案例：獵人頭公司

[31] The EDPB plans to provide further guidance in relation to clinical trials in the context of its forthcoming Guidelines on processing of personal data for medical and scientific research purposes.
EDPB 計畫在即將發出關於為醫學及科學研究目的運用個人資料的指引中，提供關於臨床試驗的進一步指引。

Company X helps Company Y in recruiting new staff- with its famous value-added service "global matchz". Company X looks for suitable candidates both among the CVs received directly by Company Y and those it already has in its own database. Such database is created and managed by Company X on its own. This ensures that Company X enhances the matching between job offers and job seekers, thus increasing its revenues. Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable candidates based on converging decisions: the decision to create and manage the service “global matchz” for Company X and the decision of Company Y to enrich the database with the CVs it directly receives. Such decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates to take place. Therefore, in this particular case they should be considered as joint controllers of such processing. However, Company X is the sole controller of the processing necessary to manage its database and Company Y is the sole controller of the subsequent hiring processing for its own purpose (organisation of interviews, conclusion of the contract and management of HR data).
X 公司以其著名的加值服務「全球 matchz」協助 Y 公司招聘新員工。X 公司從 Y 公司直接收到的履歷和它自己資料庫已有的履歷中尋找合適的人選。該資料庫由 X 公司自己建立和管理。這確保 X 公司提高工作和求職者之間的配對機會，因而增加它的收入。即使他們並未正式一起作決定，但 X 和 Y 公司基於找到合適人選的共同目的而共同參與運用過程：X 公司創立和管理「全球 matchz」服務的決定和 Y 公司以它直接收到的履歷來豐富資料庫的決定。這些決定相輔相成，對於尋找合適人選的過程是不可分割和必要的。因此，在這種特殊情況下，它們應被視為該運用的共同控管者。但是，X 公司是管理其資料庫所需過程的唯一控管者，而 Y 公司是為其自身目的（面試安排、合約簽訂和人力資源資料管理）的後續招聘過程的唯一控管者。

Example: Analysis of health data
案例：健康資料分析

Company ABC, the developer of a blood pressure monitoring app and Company XYZ, a provider of apps for medical professionals, both wish to examine how blood pressure changes can help predict certain diseases. The companies decide to set up a joint project and reach out to Hospital DEF to become involved as well.
血壓監測應用程式開發商 ABC 公司和醫療專業人士專用應用程式提供商 XYZ 公司，都希望研究血壓變化如何幫助預測某些疾病。二家公司決定成立一個聯合計畫，並與 DEF 醫院聯絡，以期他們也參與。

The personal data that will be processed in this project consists of personal data which Company ABC, Hospital DEF and Company XYZ are separately processing as individual controllers. The decision to process this data to assess blood pressure changes is taken jointly by the three actors. Company ABC, Hospital DEF and Company XYZ have jointly determined the purposes of processing. Company XYZ takes the initiative to propose the essential means of processing. Both Company ABC and the Hospital DEF accept these essential means after they as well were involved in developing some of the features of the app so that the results can be sufficiently used by them. The three organizations thus agree on having a common purpose for the processing which is the assessment of how blood pressure changes can help predict certain diseases. Once the research is completed, Company ABC, Hospital DEF and Company XYZ may benefit from the assessment by using its results in their own activities. For all these reasons, they qualify as joint controllers for this specific joint processing.
這個計畫將運用的個人資料包括 ABC 公司、DEF 醫院和 XYZ 公司作為個別控管者分別運用的個人資料。運用這些資料以評估血壓變化的決定由三個行為者共同做出。ABC 公司、DEF 醫院 XYZ 公司共同決定運用的目的。XYZ 公司主動提議運用的主要方式。ABC 公司和 DEF 醫院在參與開發應用程式的某些功能後，都接受了這些主要方式，以便他們可以充分使用。因此，這三個組織同意運用的共同目的是評估血壓變化如何有助預測某些疾病。一旦研究完成，ABC 公司、DEF 醫院和 XYZ 公司可能會透過在他們自己的活動中使用評估結果而從中獲益。因為這些理由，他們有資格成為此特定共同運用的共同控管者

If Company XYZ had been simply asked by the others to perform this assessment without having any purpose of their own and merely been processing data on behalf of the others, Company XYZ would qualify as a processor even if it was entrusted with the determination of the non-essential means.
如果 XYZ 公司只是被其他人要求執行此評估而沒有任何自己的目的，且只是代表其他人運用資料，則 XYZ 公司將有資格成為受託運用者，即使它被委託決定的是非必要方式。

3.2.3 Situations where there is no joint controllership
3.2.3 沒有共同控管的情況

69. The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification

of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership.
多個行為者參與同一個運用的事實並不意味著他們一定是該運用的共同控管者。並非所有的合夥關係、合作或協作都意指共同控管者的資格，因為這種資格需要對每個運用以及每個實體在每個運用中的確切角色進行逐案分析。以下案例提供了沒有共同控管的部分案例。

70. For example, the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers.
例如，沒有共同決定的目的或共同決定運用方式的二個實體間交換相同的資料或成套資料，應被視為不同控管者之間的資料傳輸。

Example: Transmission of employee data to tax authorities
案例：傳送員工資料給稅務機關

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.
A 公司為了管理薪資、健康保險等目的而蒐集和運用其員工的個人資料。法律規定公司有義務將所有有關薪資的資料送交稅務機關以加強財務控制。

In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.
在這種情況下，即使公司和稅務機關運用相同的薪資資料，但沒有共同決定資料運用目的和方式，結果是，這二個實體有資格成為二個獨立的資料控管者。

71. Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.
在多個實體使用共享資料庫或公共基礎設施的情況下，如果每個實體獨立決定自己的目的，也可以排除共同控管。

Example: Marketing operations in a group of companies using a shared database:
案例：企業集團公司的行銷活動中使用共享資料庫

A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.
企業集團公司使用相同的資料庫來管理客戶和潛在客戶。這樣的資料庫由母公司的伺服器代管，母公司因此是這些公司在資料儲存方面的受託運用者。集團的每個實體輸入自己的客戶和潛在客戶的資料，且只為自身目的運用這些資料。此外，每個實體單獨決定他們的客戶和潛在客戶資料的存取、留存期限、更正或刪除。他們不能存取或使用彼此的資料。只因為這些公司使用共享集團資料庫並不必然形成共同控管。因此在這種情況下，每家公司都是獨立的控管者。

Example: Independent controllers when using a shared infrastructure
案例：使用共享基礎建設之獨立控管者

Company XYZ hosts a database and makes it available to other companies to process and host personal data about their employees. Company XYZ is a processor in relation to the processing and storage of other companies' employees as these operations are performed on behalf and according to the instructions of these other companies. In addition, the other companies process the data without any involvement from Company XYZ and for purposes which are not in any way shared by Company XYZ.
XYZ 公司代管一資料庫，並提供給其他公司運用和代管他們的員工個人資料。XYZ 公司是有關其他公司員工的運用和儲存的受託運用者，因為這些工作是代表其他公司並依據其他公司的指示而執行。此外，其他公司在沒有 XYZ 公司的任何參與下運用資料，並且是為了絕不會與 XYZ 公司共享的目的。

72. Also, there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers.

此外，在某些情況下，不同的行為人在一系列操作中連續運用相同的個人資料，每個行為人在系列操作中都有獨立的目的和獨立的方式。在沒有共同參與決定同一運用操作或一組操作的目的和方式的情況下，必須排除共同控管，並且必須將各行為人視為連續獨立控管者。

Example: Statistical analysis for a task of public interest
案例：為公眾利益的統計分析

A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A.
公務機關（A 機關）的法律任務是對國家就業率的發展狀況進行相關分析和統計。為此，許多其他公共實體依法要向 A 機關揭露特定資料。A 機關決定使用特定系統運用資料，包括蒐集資料。這也意味著其他單位有義務使用該系統揭露資料。在這種情況下，在不影響法律賦予的任何角色下，為了分析和統計系統中已運用的就業率，A 機關將是運用的唯一控管者，因為 A 機關決定運用的目的，並已決定如何安排運用工作。當然，其他公共實體作為自己運用活動的控管者，有責任確保他們之前運用的資料正確，然後將這些資料揭露給 A 機關。

4 DEFINITION OF PROCESSOR
4 受託運用者的定義

73. A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "*a natural or legal person, public authority, agency or other body*". This means that there is in principle no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual.

第 4(8)條將受託運用者定義為代表控管者運用個人資料的自然人或法人、公務機關、機構或另一個團體。與控管者的定義類似，受託運用者的定義預設了廣義的行為人－它可以是「自然人或法人、公務機關、機構或另一個團體」。這表示，原則上對哪種類型的行為人可以擔任受託運用者的角色沒有限制。可以是組織，也可以是個人。

74. The GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.
GDPR 制定了直接適用於受託運用者的義務，本指引第二部分第 1 節有進一步規定。如果，受託運用者未能遵守此類義務，或者其行為超出或違反控管者的合法指示，則受託運用者可能會被追究責任或遭罰款。

75. Processing of personal data can involve multiple processors. For example, a controller may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors). A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors ("sub processor(s)"). The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended.
個人資料的運用可能涉及多個受託運用者。例如，控管者自己可能透過在運用的不同階段讓不同的受託運用者參與（多個受託運用者）選擇直接委任多個受託運用者。控管者也可能決定委任一名受託運用者，而後者又在控管者的授權下委任一個或多個其他受託運用者(「複受託運用者」)。委託給受託運用者的運用活動可能僅限於非常具體的任務或情況，或者一般和廣泛的委託。

76. Two basic conditions for qualifying as processor are:
有資格成為受託運用者的二個基本條件是：

a) being *a separate entity* in relation to the controller and
與控管者有關的獨立實體，並且

b) processing personal data *on the controller's behalf*.
代表控管者運用個人資料。

77. *A separate entity* means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a

department within a company cannot generally be a processor to another department within the same entity.
獨立實體是指控管者決定將全部或部分運用活動委託給外部組織。在公司集團中，一家公司可以是另一家擔任控管者的公司的受託運用者，因為二家公司都是獨立的實體。另一方面，公司內的一個部門通常不能成為同一實體內另一個部門的受託運用者。

78. If the controller decides to process data itself, using its own resources within its organisation, for example through its own staff, this is not a processor situation. Employees and other persons that are acting under the direct authority of the controller, such as temporarily employed staff, are not to be seen as processors since they will process personal data as a part of the controller's entity. In accordance with Article 29, they are also bound by the controller's instructions.
如果控管者決定自己運用資料，使用自己組織內的資源，例如，透過自己的員工，則這不是受託運用者的情形。在控管者的直接授權下行事的員工和其他人（例如，派遣人員）不應被視為受託運用者，因為他們是以控管者實體的一部分在運用個人資料。依據第 29 條，他們也要遵守控管者的指示。

79. *Processing personal data on the controller's behalf* firstly requires that the separate entity processes personal data for the benefit of the controller. In Article 4(2), processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction. The concept of "processing" is further described above under 2.1.5.
「代表控管者運用個人資料」首先要求獨立實體為控管者的利益運用個人資料。在第 4(2)條中，運用被定義為一個概念，包括從蒐集、儲存和諮詢到使用、傳播或以其他方式提供和銷毀的各種操作。「運用」的概念於上述 2.1.5 有進一步的描述。

80. Secondly, the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting "on behalf of" means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the Regulation will be derived from the controller's activity and the processor must not process the data otherwise than according to the controller's instructions. Even so, as described above, the controller's instructions may still leave a certain degree of discretion about how to best

serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means.[32]
其次，除在控管者直接授權或控制下進行外，運用必須代表控管者進行。「代表」意味著為某人利益而做，這讓人想起「委託」的法律概念。在資料保護法裡，至少在運用目的和方法的必要元素方面，要求受託運用者執行控管者給的指示。依據規則第 6 條（及可能相關的第 9 條）運用的合法性將來自控管者的活動，受託運用者除了依據控管者的指示外，不得運用資料。即便如此，如上所述，控管者的指示仍可能在如何最符合控管者的利益方面留下一定程度的自由裁量權，允許受託運用者選擇最合適的技術和組織方法。

81. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.
「代表」也意味著受託運用者不得為自己的目的進行運用。依據第 28(10)條的規定，受託運用者超越控管者的指示並開始決定自己的運用目的和方式，就違反了 GDPR 的規定。受託運用者將被視為該運用的控管者，並可能因超越控管者的指示而受到制裁。

Example: Service provider referred to as data processor but acting as controller
案例：服務提供者被稱為資料受託運用者但擔任控管者

Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, such as developing their own business activity. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.
服務提供者 MarketinZ 為許多公司提供促銷廣告和行銷服務。GoodProductZ 公司與 MarketinZ 簽訂合約，依據該合約，後者為

[32] See section 2.1.4 describing the distinction between essential and non-essential means.
見第 2.1.4 節描述必要與非必要方法的區別。

GoodProductZ 客戶提供商業廣告，而被稱為受託運用者。然而，MarketinZ 決定將 GoodProducts 的客戶資料庫用於 GoodProducts 廣告以外的其他目的，例如開發自己的業務活動。增加額外目的而移轉資料的決定將 MarketinZ 轉換為這組運用操作的資料控管者，且為此目的進行的運用將構成違反 GDPR。

82. The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor.[33] A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing.
EDPB 回顧，並非每個在提供服務的過程中運用個人資料的服務提供商都是 GDPR 定義的「受託運用者」。受託運用者的角色並非源於運用資料的實體種類，而是源於其在特定環境中的具體活動。服務性質將決定運用活動是否相當於 GDPR 意義上代表控管者運用個人資料。實際上，在所提供的服務並非專門針對個人資料運用或此類運用不構成服務的關鍵要素時，服務提供商也許能夠獨立決定為了提供服務所必需的運用目的和方式。在這種情況下，服務提供商將被視為單獨的控管者而不是受託運用者。為了確定每個實體在決定運用的目的和方式上的實際影響程度，必須個案判斷。

Example: Taxi service
案例：計程車服務

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that

[33] See also Recital 81 of the GDPR, which refers to "entrusting a processor processing activities", indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.
另見 GDPR 前言第 81 段，提及「委託受託運用者運用活動」，顯示運用活動是控管者決定要求受託運用者代表其運用個人資料時的重要部分。

should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of developing its own business activity to provide transportation services, without any instructions from CompanyABC. The taxi service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes places following a request for service from Company ABC.

計程車服務提供一個線上平台，公司可以透過該平台預訂計程車接送員工或訪客往返機場。在預約計程車時，ABC 公司會明確說明應從機場接走的員工姓名，以便司機在接機時確認員工的身分。在這種情況下，計程車服務運用員工的個人資料是其對 ABC 公司服務的一部分，但此類運用不是服務的目的。計程車服務公司將線上預約平台設計為開發自己的業務以提供運輸服務的一部分，而沒有來自 ABC 公司的任何指示。計程車服務也獨立決定其蒐集的資料類別和保存時間。因此，計程車服務本身就是一個控管者，儘管運用是在 ABC 公司提出服務要求後進行。

83. The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.

EDPB 指出，即使個人資料的運用不是服務的主要目的，如果服務的客戶實際上仍決定運用目的和方式，則服務提供者仍可能擔任受託運用者。在考慮是否將個人資料的運用委託給特定服務提供者時，控管者應仔細評估相關服務提供者是否允許他們行使足夠的控制權，同時考慮資料運用的性質、範圍、背景和目的，以及對當事人的潛在風險。

Example: Call center
案例：電話客服中心

Company X outsources its client support to Company Y who provides a call center in order to help Company X's clients with their questions. The client support service means that Company Y has to have access to

Company X client data bases. Company Y can only access data in order to provide the support that Company X has procured and they cannot process data for any other purposes than the ones stated by Company X. Company Y is to be seen as a personal data processor and a processor agreement must be concluded between Company X and Y.
X 公司將客戶支援業務外包給提供電話客服中心的 Y 公司，以幫助 X 公司的客戶解決他們的問題。客戶支援服務意味 Y 公司必須有權讀取 X 公司的客戶資料庫。Y 公司只能讀取資料以提供 X 公司採購的服務，他們不能出於 X 公司規定的目的以外的任何其他目的運用資料。Y 公司將被視為個人資料受託運用者，且 X 公司和 Y 公司必須簽訂受託運用者合約。

Example: General IT support
案例：一般資訊支援

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.
Z 公司聘請 IT 服務提供者為其 IT 系統提供一般支援，其中包括大量個人資料。存取個人資料不是支援服務的主要目的，但 IT 服務提供者在執行服務時，無可避免地將有系統地讀取個人資料。因此，Z 公司—IT 服務提供者—作為一家獨立公司，不可避免地被要求運用個人資料，即使這不是服務的主要目的—應被視為受託運用者，因此應與 IT 服務提供者簽訂受託運用者合約。

Example: IT-consultant fixing a software bug
案例：資訊顧問修補軟體錯誤

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to

prevent the IT-consultant from processing personal data in an unauthorised manner.
ABC 公司從另一家公司聘請一名 IT 專家來修復該公司正在使用的軟體中的錯誤。這名 IT 顧問並未受聘運用個人資料，ABC 公司確定對個人資料的任何讀取純屬偶然，因此實際上此種讀取將極為有限。因此，ABC 得出結論，這名 IT 專家不是受託運用者（自己也不是控管者），ABC 公司將依據 GDPR 第 32 條採取適當措施，以防止 IT 顧問在未獲授權下運用個人資料。

84. As stated above, nothing prevents the processor from offering a preliminary defined service but the controller must make the final decision to actively approve the way the processing is carried out, at least insofar as concerns the essential means of the processing. As stated above, a processor has a margin of manoeuvre as regards non-essential means, see above under sub-section 2.1.4.
如上所述，沒有什麼能阻止受託運用者提供初步定義的服務，但至少就運用的必要方式而言，控管者必須做出最後決定。如上所述，受託運用者在非必要方式有操作空間，參見上文第 2.1.4 節。

Example: Cloud service provider
案例：雲端服務提供者

A municipality has decided to use a cloud service provider for handling information in its school and education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers. The cloud service provider has offered a standardized service that is offered worldwide. The municipality however must make sure that the agreement in place complies with Article 28(3) of the GDPR, that the personal data of which it is controller are processed for the municipality's purposes only. It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.
市政府決定使用雲端服務提供者來處理學校和教育服務中的資料。雲端服務提供簡訊服務、視訊會議、文件儲存、行事曆管理、文字處理等，並且需要運用關於學童和教師的個人資料。雲端服務提供者提供了一套供應全球的標準化服務。然而，市政府必須確保合約符合 GDPR 第 28(3)條規定，控管者運用的個人資料僅為了市政府的目的。它還必須確保雲端服務提供者遵守他們關於儲存期限、資料刪除等方面的具體指示，而不管標準化服務通常提供什麼。

5 DEFINITION OF THIRD PARTY/RECIPIENT
5. 第三方／接收方的定義

85. The Regulation not only defines the concepts of controller and processor but also the concepts of recipient and third party. As opposed to the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. These can be said to be relative concepts in the sense that they describe a relation to a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means.
本規則不僅定義控管者和受託運用者的概念，也定義接收方和第三方的概念。與控管者和受託運用者的概念相反，本規則沒有規定接收方和第三方的具體義務或責任。這些可以說是相對概念，因為它們從特定角度描述與控管者或受託運用者的關係，例如，控管者或受託運用者揭露資料給接收方。從其他角度來看，個人資料的接收方和第三方很可能同時被視為控管者或受託運用者。例如，從某個角度來看是接收方或第三方的實體，就他們決定運用資料的目的和方式而言，是控管者。

Third party
第三方

86. Article 4(10) defines a "*third party*" as a natural or legal person, public authority, agency or body other than
第 4(10)條將"第三方"定義為自然人或法人、公務機關、機構或團體，而不是

- the data subject,
  當事人，
- the controller,
  控管者，
- the processor and
  受託運用者，和
- persons who, under the direct authority of the controller or processor, are authorised to process personal data.
  在控管者或受託運用者直接授權下運用個人資料的人。

87. The definition generally corresponds to the previous definition of "*third party*" in Directive 95/46/EC.
該定義大致上符合先前在指令 95/46/EC 中「第三方」的定義。

88. Whereas the terms "*personal data*", "*data subject*", "*controller*" and "*processor*" are defined in the Regulation, the concept of "*persons who, under the direct authority of the controller or processor, are authorised to process personal data*" is not. It is, however, generally understood as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data. An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing.[34]
雖然「個人資料」、「當事人」、「控管者」和「受託運用者」等名詞在本規則中有定義，但「在控管者或受託運用者直接授權下運用個人資料的人」則無。然而，它通常被理解為屬於控管者或受託運用者的法人實體的人（員工或與員工極為類似的角色，例如，經由派遣公司提供的臨時工作人員），但僅限於他們獲授權運用個人資料。員工等讀取他們無權存取的資料以及為了僱主目的以外的其他目的存取，不屬於此類。該員工應被視為與僱主進行運用有關的第三方。只要員工出於自己的目的（不同於僱主的目的）運用個人資料，他們將被視為控管者，並承擔由此產生的個人資料運用的所有後果和責任。

89. A third party thus refers to someone who, in the specific situation at hand, is not a data subject, a controller, a processor or an employee. For example, the controller may hire a processor and instruct it to transfer personal data to a third party. This third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It should be noted that, within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor.

---

[34] The employer (as original controller) could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures. [29] See also Recital 31 of the GDPR
萬一缺乏適當安全措施而產生新的資料運用時，僱主（原來的控管者）仍可能有責任。另見 GDPR 前言第 31 段。

因此，第三方指的是在特定情況下非屬當事人、控管者、受託運用者或員工的人。例如，控管者可能委任和指示受託運用者將個人資料傳輸給第三方。那麼，該第三方將被視為為自己的目的進行運用的控管者。要注意的是，在一個公司集團中，控管者或受託運用者以外的公司是第三方，即使它與作為控管者或受託運用者的公司屬於同一個集團。

Example: Cleaning services
案例：清潔服務

Company A concludes a contract with a cleaning service company to clean its offices. The cleaners are not supposed to access or otherwise process personal data. Even though they may occasionally come across such data when moving around in the office, they can carry out their task without accessing data and they are contractually prohibited to access or otherwise process personal data that Company A keeps as controller. The cleaners are not employed by Company A nor are they seen as being under the direct authority of that company. There is no intention to engage the cleaning service company or its employees to process personal data on Company A's behalf. The cleaning service company and its employees are therefore to be seen as a third party and the controller must make sure that there are adequate security measures to prevent that they have access to data and lay down a confidentiality duty in case they should accidentally come across personal data.
A 公司與一家清潔服務公司簽訂打掃辦公室的合約。清潔人員不應該存取或以其他方式運用個人資料。即使他們在辦公室走動時會偶然見到這些資料，但他們可以在不讀取資料的情況下執行任務，而且合約禁止他們讀取或以其他方式運用 A 公司作為控管者所保管的個人資料。清潔人員並非受僱於 A 公司，也不被視為受該公司直接授權。不存在聘請清潔服務公司或其員工代表 A 公司運用個人資料的意圖。因此，清潔服務公司及其員工應被視為第三方，控管者必須確保有適當安全措施防止他們讀取資料並加諸保密責任，以防萬一他們偶然見到個人資料。

Example: Company groups – parent company and subsidiaries
案例：集團公司—母公司與子公司

Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies

are part of the same group. Company ZZ will be regarded as controller for its processing of the data for statistical purposes.
X 和 Y 公司是 Z 集團的一員。X 和 Y 公司都為了管理員工的目的運用他們各自的員工資料。母公司 ZZ 決定跟所有子公司索取員工資料，以製作全集團的統計資料。在將資料從 X 和 Y 公司傳送到 ZZ 時，ZZ 將被視為第三方，儘管所有公司都屬於同一個集團。ZZ 公司將被視為為了統計目的而運用資料的控管者。

Recipient
接收方

90. Article 4(9) defines a "*recipient*" 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. Public authorities are however not to be seen as recipients when they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. tax and customs authorities, financial investigation units etc.)[35]
第 4(9)條將「接收方」定義為個人資料的揭露對象，包括自然人或法人、公務機關、機構或另一個團體，無論是否為第三方。但是，公務機關在依據歐盟或成員國法律（例如，稅務和海關當局、金融調查單位等）在特定調查範圍內接收個人資料時，不應被視為接收方。

91. The definition generally corresponds to the previous definition of "*recipient*" in Directive 95/46/EC.
該定義大體結合先前指令 95/46/EC 對於「接收方」的定義。

92. The definition covers anyone who receives personal data, whether they are a third party or not. For example, when a controller sends personal data to another entity, either a processor or a third party, this entity is a recipient. A third party recipient shall be considered a controller for any processing that it carries out for its own purpose(s) after it receives the data.
該定義涵蓋接收個人資料的任何人，無論他們是否為第三方。例如，當控管者將個人資料傳送給另一個實體（受託運用者或第三方）時，該實體就是接收方。接收資料的第三方在收到資料後，應被視為其為自身目的進行任何運用的控管者。

Example: Disclosure of data between companies
案例：公司間的資料揭露

[35] See also Recital 31 of the GDPR
另見 GDPR 前言第 31 段。

The travel agency ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation. However, the airlines, hotels and excursion providers are to be seen as recipients when receiving the personal data from ExploreMore.
旅行社 ExploreMore 依據客戶個別要求安排行程。在這項服務中，他們將客戶的個人資料傳送給航空公司、飯店和短程旅遊組織，以便他們執行各自的服務。ExploreMore，飯店、航空公司和短程旅遊提供者都被視為他們在各自服務中運用資料的控管者，彼此沒有控管者受託運用者的關係。然而，航空公司、飯店和短程旅遊提供者在收到來自 ExploreMore 的個人資料時將被視為接收方。

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES
第二部—歸因於不同角色的結果

1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR
1. 控管者與受託運用者的關係

93. A distinct new feature in the GDPR are the provisions that impose obligations directly upon processors. For example, a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3)); a processor must maintain a record of all categories of processing activities (Article 30(2)) and must implement appropriate technical and organisational measures (Article 32). A processor must also designate a data protection officer under certain conditions (Article 37) and has a duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)). Furthermore, the rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers. In this regard, the EDPB considers that Article 28(3) GDPR imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.[36]

[36] For instance, the processor should assist the controller, where necessary and upon request, in ensuring compliance with obligations relating to data protection impact assessments (Recital 95 GDPR). This needs to be reflected in the contract between the controller and the processor pursuant to Article 28(3)(f) GDPR.
例如，受託運用者應在必要且被要求時協助控管者，確認遵守資料保證影響評估的義務（GDPR 前言第 95 段）。在控管者和受託運用者依據 GDPR28(3)(f)條所訂的合約中必須反映此點要求。

GDPR 一個明顯的新特色是直接規定受託運用者義務的條文。例如，受託運用者必須確保獲得授權運用個人資料的人已承諾保密(第 28(3)條)；受託運用者必須保留各種運用活動的紀錄（第 30（2）條），並且必須實施適當的技術上和組織上措施（第 32 條）。受託運用者還必須在某些條件下指定個人資料保護長（第 37 條），且有責任在發現個人資料洩漏時立即通知控管者（第 33（2）條）。此外，傳輸資料至第三國的規定（第五章）適用於受託運用者和控管者。在這方面，EDPB 認為 GDPR 第 28(3)條直接規定受託運用者的義務，包括協助控管者確保合規的責任。

1.1Choice of the processor
1.1選擇受託運用者

94. The controller has the **duty to use "only processors providing sufficient guarantees** to implement appropriate technical and organisational measures", so that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights.[37] The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.
控管者有責任使用「提供充分保證實施適當技術和組織方式的受託運用者」，以便運用能符合 GDPR 的要求—包括運用的安全性—並確保當事人的權利受到保護。因此，控管者負責評估受託運用者提供保證之充足性，並應能證明已認真考慮 GDPR 中規定的所有要素。

95. The guarantees "provided" by the processor are actually those that the processor is able to **demonstrate to the satisfaction of the controller**, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognised international certifications, like ISO 27000 series).
受託運用者「提供」的保證實際上是受託運用者能展現以使控管者滿意的保證，因為這些是控管者在評估是否遵循其義務時可以有效考慮的唯一方式。這通常需要交換相關文件（例如，隱私政策、服務條款、運用活動記錄、記錄管理政策、資訊安全政策、外部查核報告、公認的國際認證，如 ISO 27000 系列）。

[37] Article 28(1) and Recital 81 GDPR.
GDPR 第 28(1)條和前言第 81 段。

96. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons.
控管者對保證是否充分的評估是一種風險評估，這大為依賴委託給受託運用者的運用類型而定並需個案考量運用的性質、範圍、背景和目的以及自然人的權利和自由的風險。

97. The following elements[38] should be taken into account by the controller in order to assess the sufficiency of the guarantees: the processor's **expert** knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's **reliability**; the processor's **resources**. The reputation of the processor on the market may also be a relevant factor for controllers to consider.
為了評估保證的充分，控管者應考慮以下因素：受託運用者的專業知識（例如，安全措施和個人資料侵害的相關專門技術）；受託運用者的可靠度；受託運用者的資源。受託運用者在市場上的聲譽也可能是控管者考慮的相關因素。

98. Furthermore, the adherence to an approved code of conduct or certification mechanism can be used as an element by which sufficient guarantees can be demonstrated. [39] The processors are therefore advised to inform the controller as to this circumstance, as well as to any change in such adherence.
此外，遵守眾所公認的行為準則或認證機制可以作用充分保證的證明要素。因此，建議受託運用者將這種情況及該遵守行為的任何變化通知控管者。

99. The obligation to use only processors "providing sufficient guarantees" contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate.[40]
GDPR 第 28(1)條規定僅使用「提供充分保證」的受託運用者，是一項持續性義務，不會在控管者和受託運用者簽訂合約或其他法律文件的

[38] Recital 81 GDPR.
GDPR 前言第 81 段。

[39] Article 28(5) and Recital 81 GDPR.
GDPR 第 28(1)條和前言第 81 段。

[40] See also Article 28(3)h GDPR.
另參見 GDPR 第 28(3)h 條。

那一刻結束。相反地，控管者應於適當間隔驗證受託運用者的保證，包括在適當情況下查核和檢查。

1.2Form of the contract or other legal act
1.2合約或其他法律文件的形式

100. Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law between the controller and the processor, as required by Article 28(3) GDPR.
GDPR 第 28(3)條要求，受託運用者運用個人資料，必須受控管者和受託運用者之間依據歐盟或成員國法律簽訂的合約或其他法律文件所規範。

101. Such legal act must be **in writing, including in electronic form**.[41] Therefore, non-written agreements (regardless of how thorough or effective they are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR. To avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act, in line with applicable law (e.g. contract law).
此類法律文件必須是書面形式，包括電子檔形式。因此，非書面合約（無論多麼完整或有效力）都不得視為足以符合 GDPR 第 28 條的要求。為避免難以證明合約或其他法律文件確實有效力，EDPB 建議依據所適用之法律(例如：合約法)確保法律文件中包含必要的簽名。

102. Furthermore, the contract or the other legal act under Union or Member State law must be **binding on the processor** with regard to the controller, i.e. it must establish obligations on the processor that are binding as a matter of EU or Member State law. Also it must set out the obligations of the controller. In most cases, there will be a contract, but the Regulation also refers to "other legal act", such as a national law (primary or secondary) or other legal instrument. If the legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements.
此外，依據歐盟或成員國法律簽訂的合約或其他法律文件，必須讓控管者對受託運用者具有約束力，亦即，它必須依據歐盟或成員國法律課予受託運用者具有約束力的義務，也必須規定控管者的義務。大多數情況下會有合約，但本規則也提到「其他法律文件」，例如國家法律

[41] Article 28(9) GDPR
GDPR 第 28(9)條。

（主要或次要）或其他法律文書。如果法律文件未包含所有最低要求的內容，則必須以合約或其他包含欠缺要素的法律文件加以補充。

103. Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR.[42] Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.[43] Subject to the provisions of Article 3 of the GDPR, the competent supervisory authority will be able to direct an administrative fine against both the controller and the processor, taking into account the circumstances of each individual case. Contracts that have been entered into before the date of application of the GDPR should have been updated in light of Article 28(3). The absence of such update, in order to bring a previously existing contract in line with the requirements of the GDPR, constitutes an infringement of Article 28(3).

A written contract pursuant to Article 28(3) GDPR may be embedded in a broader contract, such as a service level agreement. In order to facilitate the demonstration of compliance with the GDPR, the EDPB recommends that the elements of the contract that seek to give effect to Article 28 GDPR be clearly identified as such in one place (for example in an annex).

由於本規則明確規定簽訂書面合約的義務，若沒有其他有效的相關法律文件，這項缺失就違反 GDPR。控管者和受託運用者都有責任確保有合約或其他法律文件規範資料運用。依據 GDPR 第 3 條規定，監管機關考量個案狀況，可以對控管者和受託運用者處以行政罰鍰。在適用 GDPR 日期之前簽訂的合約，應依據第 28(3)條規定予以更新。未能更新使已簽訂的合約符合 GDPR 要求，即構成第 28(3)條規定的違反。

---

[42] The presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship. Where there is reason to believe that the contract does not correspond with reality in terms of actual control, the agreement may be set aside. Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of Article 28(3) GDPR. Moreover, in certain circumstances, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of legal basis on which every processing should be based, e.g. in respect of the communication of data between the controller and the alleged processor.

然而，有（或沒有）書面約定並非控管者–受託運用者關係存在的關鍵。如有理由認為合約與真正控管的情況不符時，該合約即可能被認定無效。相反地，沒有委託運用的書面合約，控管者–受託運用者關係仍可能存在，但這意味已違反 GDPR 第 28(3)條規定。此外，在某些情況下，控管者與受託運用者的關係未清楚定義，可能引發資料運用（例如在控管者和據稱的受託運用者間傳遞資料）缺少法律依據的問題。

[43] Article 28(3) is not only applicable to controllers. In the situation where only the processor is subject to the territorial scope of the GDPR, the obligation shall only be directly applicable to the processor, see also EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.

第 28(3)條不僅適用於控管者。在只有受託運用者是 GDPR 管轄地區的主體時，義務直接適用於受託運用者。另見 EDPB 3/2018 關於 GDPR 地區範圍的指引，第 12 頁。

依據 GDPR 第 28(3)條簽訂的書面合約可以納入更廣泛的合約，例如服務等級協議。為了便於證明遵守 GDPR 規定，EDPB 建議將使 GDPR 第 28 條生效的合約要素清楚標明於一個地方(例如：於附件)。

104. In order to comply with the duty to enter into a contract, **the controller and the processor may choose to negotiate their own contract** including all the compulsory elements **or to rely, in whole or in part, on standard** contractual **clauses in relation to obligations under Article 28**.[44]
為了履行訂立合約的義務，控管者和受託運用者可以選擇協商他們的合約，包括所有強制規定，或全部或部分採用與第 28 條有關義務的標準合約條款。

105. A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission[45] or adopted by a supervisory authority, in accordance with the consistency mechanism.[46] These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43.[47]
一套標準合約條款(SCCs)可以由委員會或監管機關依據一致性機制通過後採用。這些條款可做為依據第 42 或 43 條授予控管者或受託運用者的證明的一部分。

106. The EDPB would like to clarify that there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable for the purposes of compliance with data protection law, depending on the specific circumstances, as long as they meet the Article 28(3) requirements.

---

44 Article 28(6) GDPR. The EDPB recalls that standard contractual clauses for the purposes of compliance with Article 28 GDPR are not the same as standard contractual clauses referred to in Article 46(2). While the former further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled, the latter provide appropriate safeguards in case of transfer of personal data to a third country or an international organisation in the absence of an adequacy decision pursuant to Article 45(3).
GDPR 第 28(6)條。EDPB 回顧，為遵守 GDPR 第 28 條標準合約條款和第 46(2)條提及的標準合約條款不同。前者進一步規定並闡明如何履行第 28(3)和(4)條規定，後者則提供在沒有依據第 45(3)條適足性認定的情況下，將個人資料轉移到第三國或國際組織時的適當保護。

45 Article 28(7) GDPR.
GDPR 第 28(7)條。

46 Article 28(8) GDPR. The Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, including standard contractual clauses for the purposes of compliance with art. 28 GDPR, can be accessed here: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions
GDPR 第 28(8)條。監管機關和法院對於以一致性機制處理的議題做成的決定（詳參：https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions），包括為了遵守 GDPR 第 28 條規定而使用標準合約條款。

47 Article 28(6) GDPR.
GDPR 第 28(6)條。

EDPB 澄清，控管者和受託運用者沒有義務簽訂以 SCCs 為基礎的合約，也不一定要優先採用這種合約而不個別協商合約。為遵守資料保護法，只要符合第 28(3)條規定，依確切狀況而定，這二種選擇都可行。

107. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs. The SCCs will often leave some blank spaces to be filled in or options to be selected by the parties. Also, the SCCs will generally be embedded in a larger agreement describing the object of the contract, its financial conditions, and other agreed clauses: it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction) as long as they do not contradict, directly or indirectly, the SCCs[48] and they do not undermine the protection afforded by the GDPR and EU or Member State data protection laws.
如果各方當事人希望採用標準合約條款，合約的資料保護條款必須與 SCCs 資料保護條款相同。SCCs 通常會留下供各方填寫的一些空白區域或供各方選擇的選項。此外，SCCs 通常會內含在一份較大的合約中，該合約描述合約的目的、其財務狀況和其他同意的條款：各方可以增加附加條款（例如，適用法律和管轄權），只要他們不會直接或間接抵觸 SCCs，也不會破壞 GDPR 和歐盟或成員國資料保護法所提供的保護。

108. Contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. For instance, some service providers tend to set up standard terms and conditions, which include data processing agreements.
控管者和受託運用者之間的合約有時可能由單方草擬。起草合約的一方或多方可能取決於幾個因素，包括：各方在市場中的地位和合約權

[48] The EDPB recalls that the same degree of flexibility is allowed when the parties choose to use SCCs as appropriate safeguard for transfers to third countries pursuant to Article 46(2)(c) or Article 46(2)(d) GDPR. Recital 109 GDPR clarifies that "*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses [...] or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses*".
EDPB 回顧，當雙方依據 GDPR 第 46(2)(c)條或第 46(2)(d)條選擇使用 SCCs 作為轉移到第三國的適當保護時，有相同程度的靈活性。GDPR 前言第 109 段闡明：「控管者或受託運用者使用委員會或監管機關通過的標準資料保護條款的可能性，應使他們不得將標準資料保護條款放進範圍更大的合約，例如受託運用者與另一受託運用者之間的合約，或增加其他條款或額外保障措施，前提是它們不直接或間接牴觸標準合約條款（……）或損害當事人的基本權利或自由。應鼓勵控管者和受託運用者透過補充標準保護條款的合約承諾，提供額外保障」。

力、他們的技術專長及獲得法律服務的機會。例如，有些服務提供商傾向制定標準條款和條件，包括資料運用委託契約。

109. An agreement between the controller and processor must comply with the requirements of Article 28 GDPR in order to ensure that the processor processes personal data in compliance with the GDPR. Any such agreement should take into account the specific responsibilities of controllers and processors. Although Article 28 provides a list of points which must be addressed in any contract governing the relationship between controllers and processors it leaves room for negotiations between the parties to such contracts. In some situations a controller or a processor may be in a weaker negotiation power to customize the data protection agreement. Reliance on the standard contractual clauses adopted pursuant to Article 28 (subparagraphs 7 and 8) may contribute to rebalancing the negotiating positions and to ensure that the contracts respect the GDPR.
控管者和受託運用者之間的合約必須遵守 GDPR 第 28 條規定，以確保受託運用者運用個人資料符合 GDPR 規定。任何這類合約都必須考慮控管者和受託運用者的特定責任。雖然第 28 條提供了規範控管者和受託運用者之間關係的合約必要之點，但也提供合約當事人協商空間。在某些情況下，控管者或受託運用者可能在協商資料運用委託合約時的談判力較弱。仰賴依據第 28 條（第 7 和 8 項）制定的標準合約條款，可以重新平衡雙方的談判地位，確保合約遵守 GDPR 規定。

110. The fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. Also, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller. The mere publication of these modifications on the processor's website is not compliant with Article 28. It is however possible for the processor to suggest elements that, if accepted by the controller, become part of the instructions given.
合約及詳細的業務條款由服務提供者而不是控管者準備，這件事本身並沒有問題，也不能作為認定服務提供者應被視為控管者的充分依據。

此外，小資料控管者對上大服務提供者的合約權力不平衡，不應被視為控管者接受不符合資料保護法的合約條款的理由，也不能免除控管者的資料保護義務。控管者必須評估這些條款，並且只要它隨自己的自由意志接受它們並使用服務，它就也承擔了遵守 GDPR 的全部責任。受託運用者對標準條款和條件中包含的資料運用合約的任何修改提議都應直接通知控管者並獲得控管者的同意。只在受託運用者的網站上公布這些修改不符合第 28 條的規定。然而，受託運用者可以提出建議，如果控管者接受，則成為所給予指示的一部分。

1.3Content of the contract or other legal act
1.3合約或其他法律文件的內容

111. Before focusing on each of the detailed requirements set out by the GDPR as to the content of the contract or other legal act, some general remarks are necessary.
在關注 GDPR 對合約或其他法律文件內容提出的每一個詳細要求之前，必須先有一般性說明。

112. While the elements laid down by Article 28 of the Regulation constitute the core content of the agreement, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, **the processing agreement should not merely restate the provisions of the GDPR**: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement. Far from being a pro-forma exercise, the negotiation and stipulation of the contract are a chance to specify details regarding the processing.[49] Indeed, the "protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors [...] requires a clear allocation of the responsibilities" under the GDPR.[50]
雖然規則第 28 條規定的要素構成合約的核心內容，但合約應成為控管者和受託運用者進一步明確這些核心要素將如何在詳細說明下實施的方式。因此，運用合約不應只是重述 GDPR 的條文：而應包括更明確、具體的資訊，說明如何符合要求以及運用合約之目的的個人資料運用需要何種安全等級。合約的談判和制定完全不是形式，而是一個明確說明運用細節的機會。事實上，依據 GDPR，「保護當事人的權利和自

[49] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), p. 5.
另見 EDPB 14/2019 關於 DK SA 所提標準合約條款草案（GDPR 第 28(8)條）的意見，第 5 頁。

[50] Recital 79 GDPR.
GDPR 前言第 79 段。

由，以及控管者和受託運用者的責任和義務（……）需要明確分配責任」。

113. At the same time, the contract should **take into account "*the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject*"**.[51] Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract. At the same time, the contract should include some elements that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing: because the activity is performed on behalf of the controller, often the controller has a deeper understanding of the risks that the processing entails since the controller is aware of the circumstances in which the processing is embedded.
同時，合約應考慮「受託運用者在運用過程中的明確任務和責任，以及當事人的權利與自由的風險」。一般來說，雙方之間的合約應依據具體的資料運用活動來草擬。例如，對受委託進行僅會產生輕微風險之運用活動的受託運用者，沒有必要施予特別嚴格的保護和程序：雖然每個受託運用者都必須遵守本規則的要求，但措施和程序應依確切情況量身打造。無論如何，合約必須涵蓋第 28(3)條的所有要素。同時，合約中應包含一些可能有助於受託運用者了解運用過程中對當事人的權利和自由所產生風險的要素：由於該活動是代表控管者執行，因此控管者通常對運用所帶來的風險有更深的了解，因為控管者知道運用活動所處的環境。

114. Moving on to the **required content** of the contract or other legal act, EDPB interprets Article 28(3) in a way that it needs to set out:
接著談到合約或其他法律文件要求的內容，EDPB 解釋第 28(3)條需要闡明：

- the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;

[51] Recital 81 GDPR.
GDPR 前言第 81 段。

運用的主題（例如，人們進出高度安全設施的監視錄影畫面）。雖然運用的主題是一個廣泛的概念，但需要定得夠明確，以清楚知道運用的主題是什麼；

- the **duration**[52] of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;
運用的持續時間：確切的期間或用於確定它的標準應詳細說明；例如，可以提出運用合約之期限的參考；

- the **nature** of the processing: the type of operations performed as part of the processing (for instance: "filming", "recording", "archiving of images", ...) **and purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.
運用的性質：作為運用的一部分而執行的操作類型（例如：「拍攝」、「記錄」、「圖像存檔」……）和運用的目的（例如：偵測非法進入）。這種描述應盡可能全面，視具體運用活動而定，以便外部各方（例如監管機關）了解委託受託運用者運用的內容和風險。

- the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is "personal data pursuant to Article 4(1) GDPR" or "special categories of personal data pursuant to Article 9". In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, "information regarding health records", or "information as to whether the data subject is a member of a trade union";
個人資料的類型：這應盡可能以最詳細的方式說明（例如：個人進出設施的影像畫面）。只指出它是「依據 GDPR 第 4(1)條的個人資料」或「依據第 9 條的特種個資」是不夠的。對於特種個資，合約或法律文件至少應明確說明相關資料是哪些類型，例如，「關於健康記錄的資料」，或「關於當事人是否為工會成員的資訊」；

[52] The duration of the processing is not necessarily equivalent to the duration of the agreement (there may be legal obligations to keep the data longer or shorter).
資料運用持續時間不一定等於合約存續期間（可能有將資料保留更久或更短的法律義務）。

- the **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: “visitors”, “employees”, delivery services etc.);
  當事人的類別：這也應該以非常具體的方式說明（例如：「訪客」、「員工」、送貨服務等）；

- the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller’s obligation to provide the processor with the data mentioned in the contract, to provide and document, in writing, any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.
  控管者的義務和權利：控管者的權利在以下章節中進一步討論（例如，關於控管者進行檢查和查核的權利）。至於控管者的義務，案例包括控管者有義務提供合約中提到的資料給受託運用者，以書面形式提供和記錄與受託運用者運用資料有關的任何指令，以確保在運用之前和整個運用期間，受託運用者遵守 GDPR 中規定的受託運用者義務，以及監督運用過程，包括對受託運用者進行查核和檢查。

115. While the GDPR lists elements that always need to be included in the agreement, other relevant information may need to be included, depending on the context and the risks of the processing as well as any additional applicable requirement.
雖然 GDPR 列出了合約中必需包含的要素，但也可能需要包含其他相關訊息，此視背景環境和運用的風險，以及任何其他適用的要求而定。

1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR)
1.3.1 受託運用者應僅運用控管者以書面文件指示的資料（GDPR 28(3)(a)條）

116. The need to specify this obligation stems from the fact that the processor processes data on behalf of the controller. Controllers must provide its processors with instructions related to each processing activity. Such instructions can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc. The processor shall not go beyond what is instructed by the controller.

明確說明這一義務的必要性源於受託運用者代表控管者運用資料的事實。控管者必須提供它的受託運用者每個運用活動的相關指示。這類指示可能包括對個人資料允許和不可接受的運用、更詳細的程序、保護資料的方式等。受託運用者不得超越控管者的指示。

117. When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) (see section 1.5 below[53]).
當受託運用者未依照或超越控管者的指示運用資料，且已相當於決定運用的目的和方式時，受託運用者就違反其義務，且依據第 28(10)條甚至會被視為該運用的控管者（見以下第 1.5 節）。

118. The instructions issued by the controller must be **documented**, it is recommended to include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, they can be provided in any written form (e.g. e-mail), as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act.
控管者給予的指示必須記錄下來，因此建議合約或其他法律文件的附件中包含一個提供進一步指示的程序和範本。或者，只要可以記錄這類說明，它們可以是任何書面形式（例如電子郵件）。無論如何，為避免難以證明控管者的指示已被適當記錄，EDPB 建議將這類指示與合約或其他法律文件一起保存。

119. The duty for the processor to refrain from any processing activity not based on the controller's instructions also applies to **transfers** of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.
受託運用者避免進行任何非依控管者指示之運用活動的義務也適用於將個人資料轉移到第三國或國際組織的情況。考量到 GDPR 第五章的規定，合約應詳細說明轉移到第三國或國際組織的規定。

120. The EDPB recommends that controller pay due attention to this specific point especially when the processor is going to delegate some processing activities to other processors, and when the processor has divisions or units

[53] See Part II, sub-section 1.5 ("Processor determining purposes and means of processing").
見第二部分第 1.5 節（「受託運用者決定運用目的和方式」）。

located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.
EDPB 建議控管者應當注意這一點，尤其是當受託運用者將某些運用活動委託給其他受託運用者時，以及受託運用者在第三國設有分支機構或單位時。如果控管者的指示不允許轉移或揭露給第三國，受託運用者就不得將運用指派給第三國的次受託人，也不得在他其中一個非歐盟的分支機構運用資料。

121. A processor may process data other than on documented instructions of the controller **when the processor is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject**. This provision further reveals the importance of carefully negotiating and drafting data processing agreements, as, for example, legal advice may need to be sought by either party as to the existence of any such legal requirement. This needs to be done in a timely fashion, as the processor has an obligation to inform the controller of such requirement before starting the processing. Only when that same (EU or Member State) law forbids the processor to inform the controller on "important grounds of public interest", there is no such information obligation. In any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 48 of the GDPR.
當受託運用者是依據歐盟法律或受託運用者所屬成員國法律運用和／或轉移個人資料時，受託運用者可以不依照控管者的書面指示運用資料。這個條款進一步揭露詳細談判和草擬資料運用合約的重要性，例如，任何一方都可能需要就任何此類法律要求的存在尋求法律意見。這需要及時完成，因為受託運用者有義務在開始運用之前通知控管者有這樣的要求。只有當同樣的（歐盟或成員國）法律禁止受託運用者以「公共利益的重要理由」通知控管者時，才沒有此類義務。無論如何，只有在歐盟法律（包括依據 GDPR 第 48 條）授權下，才能進行轉移或揭露。

1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)
1.3.2 受託運用者必須確定獲得授權運用個人資料者已承諾保密或有適當法定保密義務（GDPR 第 28（3）（b）條）

122. The contract must say that the processor needs to ensure that anyone it allows to process the personal data is committed to confidentiality. This may

occur either via a specific contractual agreement, or due to statutory obligations already in place.
合約必須說明受託運用者需確保任何它允許運用個人資料者承諾保密。此可透過特定合約協議，或因已經存在的法定義務而履行。

123. The broad concept of "persons authorised to process the personal data" includes employees and temporary workers. Generally speaking, the processor should make the personal data available only to the employees who actually need them to perform tasks for which processor was hired by the controller.
「被授權運用個人資料者」的廣義概念包括員工和派遣人員。一般而言，受託運用者應僅將個人資料提供給實際需要以執行控管者交付受託運用者任務的員工。

124. The commitment or obligation of confidentiality must be "appropriate", i.e. it must effectively forbid the authorised person from disclosing any confidential information without authorisation, and it must be sufficiently broad so as to encompass all the personal data processed on behalf of the controller as well as the conditions under which the personal data are processed.
保密承諾或義務必須是「適當的」，即它必須有效禁止被授權人未經授權揭露任何機密訊息，且它必須足夠廣泛，以涵蓋代表控管者運用的所有個人資料以及運用個人資料之情況。

1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)
1.3.3 受託運用者必須依 32 條（GDPR 第 28（3）（c）條）規定採取一切方法

125. Article 32 requires the controller and the processor to implement appropriate technical and organisational security measures. While this obligation is already directly imposed on the processor whose processing operations fall within the scope of the GDPR, the duty to take all measures required pursuant to Article 32 still needs to be reflected in the contract concerning the processing activities entrusted by the controller.
第 32 條要求控管者和受託運用者實施適當的技術和組織安全措施。雖然這一義務已經直接施加其運用符合 GDPR 範圍內的受託運用者身上，但依據第 32 條的要求採取所有措施的義務，仍需反映在與控管者委託的運用活動有關的合約中。

126. As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted**, an obligation on the**

processor to obtain the controller's approval before making changes, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR.

如前所述，運用合約不應只是重述 GDPR 的條文。合約需要包括或參考有關將採取的安全措施的資訊、受託運用者在改動之前應獲得控管者同意的義務，以及定期審查安全措施，以確保其在風險方面的適用性，這可能會隨著時間而演變。合約中包含的安全措施相關訊息的詳細程度，必須使控管者能依據 GDPR 第 32(1)條評估措施的適用性。此外，為了使控管者能遵守它依據 GDPR 第 5(2)條和第 24 條有關施予受託運用者之安全措施的問責義務，該描述也是必要的。受託運用者協助控管者並提供證明合規性所需的所有資訊的相應義務可以從 GDPR 第 28.3(f)和(h)條中推斷出來。

127. The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.

控管者提供給受託運用者關於要執行之措施的指示程度取決於具體狀況。在某些情況下，控管者可能對要實施的安全措施給出清楚而詳細的描述。在其他情況時，控管者可能描述要達成的最低安全目標，同時要求受託運用者提出實施明確安全措施的方法。無論如何，控管者必須對受託運用者描述運用活動和安全目標（依據控管者的風險評估），並同意受託運用者提出的措施。這可能包含在合約的附件中。控管者

對於安全措施之主要功能應行使決策權，無論是透過明確列出措施還是同意受託運用者提出的措施。

1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).
受託運用者委託另一位受託運用者時必須遵守第 28（2）和 28（4）條提及的條件（GDPR 第 28（3）（d）條）

128. The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation and whether this authorisation will be specific or general. In case of general authorisation, the processor has to inform the controller of any change of subprocessors under a written authorisation, and give the controller the opportunity to object. It is recommended that the contract set out the process for this. It should be noted that the processor's duty to inform the controller of any change of sub-processors implies that the processor actively indicates or flags such changes toward the controller. [54] Also, where specific authorisation is required, the contract should set out the process for obtaining such authorisation.
合約必須明確說明，未經控管者事先書面授權，受託運用者不得聘請其他受託運用者，以及該授權是特定還是一般性。如果是一般授權，受託運用者必須將書面授權的次受託人的任何變動通知控管者，並給控管者反對的機會。建議在合約中訂定此規定的流程。應注意的是，受託運用者有責任將次受託人的任何變化通知控管者，意指受託運用者應主動向控管者表明或標記這樣的變化。此外，在需要明確授權時，合約應規定獲得此類授權的流程。

129. When the processor engages another processor, a contract must be put in place between them, imposing the same data protection obligations as those imposed on the original processor or these obligations must be imposed by another legal act under Union or Member State law. This includes the obligation under Article 28(3)(h) to allow for and contribute to audits by the controller or another auditor mandated by the controller.[55] The processor is

---

[54] In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).
相反地，對於受託運用者來說，只提供控管者對可能不時更新的次受託人名單的一般資訊，而不指明有意複委託的每個新的次受託人是不夠的。換句話說，受託運用者必須主動通知控管者名單的任何更改（特別是有意複委託的每個新的次受託人）。

[55] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 44.
另見 EDPB 關於 DK SA 所提 14/2019 標準合約條款草案（GDPR 第 28(8)條）的意見，2019 年 7 月 9 日，第 44 段。

liable to the controller for the other processors' compliance with data protection obligations (for further details on the recommended content of the agreement see section1.6 below[56]).
當受託運用者聘請另一個受託運用者時，他們之間必須簽訂合約，規定與原始受託運用者相同的個人資料保護義務，或者這些義務必須依據歐盟或成員國法律規定的另一法律行為規定。這包括第 28(3)(h)條規定的義務，允許並協助控管者查核或控管者委託的另一位審計員進行查核。受託運用者要為其他受託運用者遵守個人資料保護的義務向控管者負責（有關更多合約建議內容的詳情，請參見以下第 1.6 節）。

1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR).
1.3.5 受託運用者必須協助控管者履行其義務以回應當事人行使權利的要求（GDPR 第 28（3）（e）條）

130. While ensuring that data subjects requests are dealt with is up to the controller, the contract must stipulate that the processor has an obligation to provide assistance "by appropriate technical and organisational measures, insofar as this is possible". The nature of this assistance may vary greatly "taking into account the nature of the processing" and depending on the type of activity entrusted to the processor. The details concerning the assistance to be provided by the processor should be included in the contract or in an annex thereto.
雖然確保當事人的請求得到解決是取決於控管者，但合約必須規定受託運用者有義務「在可能的情況下，透過適當的技術和組織措施」提供協助。「考慮到運用的性質」並視委託給受託運用者的活動類型而定，這種協助的性質可能有很大的差異。有關受託運用者提供協助的詳細資訊應包含在合約或其附件中。

131. While the assistance may simply consist in promptly forwarding any request received, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data.
雖然，協助可能只是迅速轉發收到的任何要求，但在某些情況下，受託運用者將被賦予更具體的技術職責，尤其是它處於獲取和管理個人資料的地位時。

[56] See Part II, sub-section 1.6 ("Sub-processors").
見第二部分第 1.6 節（「次受託者」）。

132. It is crucial to bear in mind that, although the practical management of individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.
重要的是要記住，雖然實際管理個人要求的工作可以外包給受託運用者，但控管者有責任遵從此類要求。因此，評估當事人的要求是否可以接受和／或是否符合 GDPR 的規定，應由控管者依據個案或在運用過程開始前，藉由合約給受託運用者清楚指示來執行。此外，控管者不能基於受託運用者必須提供必要資訊的事實來延長第三章規定的最後期限。

1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).
1.3.6 受託運用者必須協助控管者確實遵守依第 32 到 36 條（GDPR 第 28（3）（f）條）規定的義務

133. It is necessary for the contract to avoid merely restating these duties of assistance: **the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations**. For example, procedures and template forms may be added in the annexes to the agreement, allowing the processor to provide the controller with all the necessary information.
合約必須避免只是重述這些協助義務：合約應包含如何要求受託運用者協助控管者履行所列義務的細節。例如，合約的附件中可加入程序和範本表格，讓受託運用者能提供所有必要資訊給控管者。

134. The type and degree of assistance to be provided by the processor may vary widely "*taking into account the nature of processing and the information available to the processor*". The controller must adequately inform the processor as to the risk involved in the processing and as to any other circumstance that may help the processor meet its duty.
「考量到運用的性質和受託運用者可獲得的資訊」，受託運用者提供的協助類型和程度可能有很大差異。控管者必須充分告知受託運用者運用過程中涉及的風險，以及任何其他可能有助受託運用者履行職責的情況。

135. Moving on to the specific obligations, the processor has, first, a duty to assist the controller in meeting the obligation to adopt adequate technical and organisational measures to ensure security of processing.[57] While this may overlap, to some extent, with the requirement that the processor itself adopts adequate security measures, where the processing operations of the processor fall within the scope of the GDPR, they remain two distinct obligations, since one refers to the processor's own measures and the other refers to the controller's.
接著談到具體義務，首先，受託運用者有義務協助控管者履行義務，採取適當的技上和組織上措施，以確保資料運用的安全性。雖然，受託運用者的資料運用落在 GDPR 範圍時，某種程度可能與受託運用者本身採取適當安全措施的要求重疊，但它們仍然是二個明顯不同的義務，因為一個是受託運用者自己的措施，而另一個是控管者的措施。

136. Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach affecting the processor's or a sub-processor's facilities / IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority.[58] The GDPR requires that the controller notify a breach without undue delay in order to minimize the harm for individuals and to maximize the possibility to address the breach in an adequate manner. Thus, the processor's notification to the data controller should also take place without undue delay.[59] Depending on the specific features of the processing entrusted to the processor, it may be appropriate for the parties to include in the contract a specific timeframe (e.g. number of hours) by which the processor should notify the controller, as well as the point of contact for such notifications, the modality and the minimum content expected by the controller.[60] The contractual arrangement between the controller and the processor may also include an authorisation and a requirement for the processor to directly notify a data breach in accordance with Articles 33 and 34, but the legal responsibility for the notification

---

[57] Article 32 GDPR.
GDPR 第 32 條。

[58] Article 33(3) GDPR.
GDPR 第 33(3)條。

[59] For more information, see the Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 13-14.
更多資訊請見 2016/679 關於個人資料外洩通知，第 WP250 號指引修訂一版，2018 年 2 月 6 日，第 13-14 頁。

[60] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 40.
另見 EDPB 對 DK SA 所提 14/2019 標準化合約條款草案（GDPR 第 28(8)條）的意見，2019 年 7 月 9 日，第 40 段。

remains with the controller.[61] If the processor does notify a data breach directly to the supervisory authority, and inform data subjects in accordance with Article 33 and 34, the processor must also inform the controller and provide the controller with copies of the notification and information to data subjects.

其次，受託運用者必須協助控管者履行將個人資料外洩事件通報監管機關和當事人的義務。當受託運用者發現影響受託運用者或次受託人的設施／IT 系統的個人資料外洩時必須通知控管者，並幫助控管者取得需在給監管機關的報告中說明的資訊。GDPR 要求控管者不得無故拖延通知外洩事件，以便將對個人的傷害減到最低，並儘可能以適當方式解決外洩事件。因此，受託運用者給資料控管者的通知也應該不得無故拖延。依據委託給受託運用者的運用特點，雙方可在合約中包含受託運用者應通知控管者的具體時間範圍（例如，小時數）以及這類通知的聯絡人，控管者預期的形式和至少要包含的內容。控管者與受託運用者之間的合約還可能包含授權和要求受託運用者依據第 33 和 34 條直接通知資料外洩，但通知的法律責任仍由控管者承擔。如果，受託運用者確實直接向監管機關通報資料外洩事件，並按照第 33 和 34 條的規定通知當事人，則受託運用者還必須通知控管者並提供控管者通知的副本和給當事人的資料。

137. Furthermore, the processor must also assist the controller in carrying out data protection impact assessments when required, and in consulting the supervisory authority when the outcome reveals that there is a high risk that cannot be mitigated.

此外，受託運用者必須在需要時協助控管者進行資料保護影響評估，並在結果顯示有無法降低的高風險時諮詢監管機關。

138. The duty of assistance does not consist in a shift of responsibility, as those obligations are imposed on the controller. For instance, although the data protection impact assessment can in practice be carried out by a processor, the controller remains accountable for the duty to carry out the assessment[62] and the processor is only required to assist the controller "where necessary and upon request."[63] As a result, the controller is the one that must take the initiative to perform the data protection impact assessment, not the processor.

---

[61] Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 14.
依據第 WP250 號修訂一版 2016/679 關於個人資料侵害事件通知的指引，2018 年 2 月，14 頁。

[62] 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, WP 248 rev.01, p. 14
資料保護工作小組第 29 條，資料保護影響評估指引及判斷為本指引之目的，資料運用是否「可能帶來高風險」，第 WP 248 號指引修訂一版，第 14 頁。

[63] Recital 95 GDPR.

協助義務不是責任轉移，因為那些義務是由控管者所承擔的。例如，雖然資料保護影響評估實際上可由受託運用者執行，但控管者仍應對進行評估的義務負責，受託運用者只需在「必要和接到請求時」協助控管者。因此，控管者是必須主動執行資料保護影響評估的人，而不是受託運用者。

1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).
1.3.7 終止運用活動時，在控管者選擇下，受託運用者必須刪除或把所有個人資料歸還控管者並刪除現有副本（GDPR 第 28（3）（g）條）

139. The contractual terms are meant to ensure that the personal data are subject to appropriate protection after the end of the "provision of services related to the processing": it is therefore up to the controller to decide what the processor should do with regard to the personal data.
合約條款旨在確保個人資料在「提供與運用相關的服務」結束後受到適當的保護：因此，要由控管者決定受託運用者應該如何運用個人資料。

140. The controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing. The contract should specify the process for providing such instructions.
控管者可以一開始就決定個人資料是要刪除或歸還，透過在合約中明確規定，以書面通訊及時發送給受託運用者。合約或其他法律文件應顯示資料控管者在提供與運用相關的服務結束之前可以改變選擇。合約應明確說明提供此類指示的流程。

141. If the controller chooses that the personal data be deleted, the processor should ensure that the deletion is performed in a secure manner, also in order to comply with Article 32 GDPR. The processor should confirm to the controller that the deletion has been completed within an agreed timescale and in an agreed manner.
如果控管者選擇刪除個人資料，則受託運用者應確保以安全的方式執行刪除，亦確保遵守 GDPR 第 32 條的規定。受託運用者應與控管者確認已在約定的時間範圍內以約定的方式完成刪除。

GDPR 前言第 95 段。

142. The processor must delete all existing copies of the data, unless EU or Member State law requires further storage. If the processor or controller is aware of any such legal requirement, it should inform the other party as soon as possible.
受託運用者必須刪除所有現有的資料副本，除非歐盟或成員國法律要求另外儲存。如果受託運用者或控管者知道任何此類法律要求，應盡快通知另一方。

1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).
1.3.8 受託運用者必須提供控管者所有證明遵守第 28 條規定義務所需的資訊，並允許和協助由控管者或另一名由控管者委任的審計人員進行查核，包括檢查（GDPR 第 28（3）（h）條）

143. The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing. For instance, the relevant portions of the processor's records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, retention of data, data location, transfers of data, access to data and recipients of data, sub-processors used, etc.
合約應詳細說明受託運用者與控管者之間資訊流動的頻率和方式，以讓控管者充分了解運用過程的細節。例如，受託運用者的運用活動記錄之相關部分可能與控管者共享。受託運用者應提供有關如何代表控管者執行運用活動的所有資料。這些資料應包括所使用系統的功能、安全措施、保留資料、資料位置、資料轉移、資料存取和資料接收者、選用的次受託人等。

144. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller.
合約中還應載明控管者或控管者委託的另一位審計員執行檢查和協助查核的能力和義務。
The GDPR specifies the inspections and audits are carried out by the controller or by a third party mandated by the controller. The goal of such audit is ensuring that the controller has all information concerning the processing activity performed on its behalf and the guarantees provided by

the processor. The processor may suggest the choice of a specific auditor, but the final decision has to be left to the controller according to Article 28(3)(h) of the GDPR.[64] Additionally, even where the inspection is performed by an auditor proposed by the processor, the controller retains the right to contest the scope, methodology and results of the inspection.[65]

GDPR 明定檢查和查核由控管者或控管者授權的第三方執行。該審計的目的是確保控管者擁有關於代表其執行的運用活動的所有資料以及受託運用者提供的保證。受託運用者可能會建議選擇特定的審計員，但依據 GDPR 第 28(3)(h)條，最終決定必須留給控管者。此外，即使檢查是由受託運用者建議的審計員執行，控管者仍保留對檢查的範圍、方法和結果提出異議的權利。

The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises, as well as which type of audit or inspection (remote / on-site / other way to gather the necessary information) would be needed and appropriate in the specific case also taking into account security concerns; the final choice on this is to be taken by the controller. Following the results of the inspection, the controller should be able to request the processor to take subsequent measures, e.g. to remedy shortcomings and gaps identified.[66] Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see section 1.6 below[67]).

各方應本誠信原則合作，並評估是否以及何時需要對受託運用者的工作場所進行查核，以及在特定情況下所需和適當的查核或檢查類型（遠距／現場／其他方式以蒐集必要的資料），同時考慮到安全問題；此事的最終選擇在控管者。依據檢查結果，控管者能夠要求受託運用者採取後續措施，例如，彌補發現的缺點和差距。同樣地，應就受託運用者和控管者對次受託人的檢查制定具體程序（見以下第 1.6 節）。

145. The issue of the allocation of costs between a controller and a processor concerning audits is not covered by the GDPR and is subject to commercial considerations. However, Article 28 (3)(h) requires that the contract include an obligation for the processor to make available all information necessary

---

64 See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 43.
見 EDPB -歐盟資料保護監督機關就控管者與受託運用者標準合約條款的共同意見 1/2021，第 43 段。

65 See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
見針對 DK SA 所提 14/2019 標準化合約條款草案（GDPR 第 28(8)條）的意見，第 43 段。

66 See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.
見針對 DK SA 所提 14/2019 標準化合約條款草案（GDPR 第 28(8)條）的意見，第 43 段。

67 See Part II, sub-section 1.6 ("Sub-processors").
見第二部分第 1.6 節（「次受託人」）。

to the controller and an obligation to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. This means in practice that parties should not insert in the contract clauses envisaging the payment of costs or fees that would be clearly disproportionate or excessive, thus having a dissuasive effect on one of the parties. Such clauses would indeed imply that the rights and obligations set out in Article 28(3)(h) would never be exercised in practice and would become purely theoretical whereas they form an integral part of the data protection safeguards envisaged under Article 28 GDPR.
GDPR 未涵蓋控管者和受託運用者之間有關審計的費用分配議題，這是出於商業考量。但是，第 28(3)(h)條要求合約中包含受託運用者提供控管者所有必要資料的義務，以及允許並協助控管者或控管者委託的另一位審計員進行查核（包括檢查）的義務。這表示實際上，當事人不應在合約中增加預設支付明顯不相稱或過多成本或費用的條款，因而對其中一方產生遏阻效果。此類條款確實意味著第 28(3)(h)條中規定的權利和義務永遠不會實際行使，並且將成為純粹的理論，而它們是 GDPR 第 28 條預設的資料保護保障措施的內含。

1.4Instructions infringing data protection law
1.4違反資料保護法的指示

146. According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.
依據第 28(3)條，如果受託運用者認為指令違反 GDPR 或其他歐盟或成員國的資料保護規定，則必須立即通知控管者。

147. Indeed, the processor has a duty to comply with the controller's instructions, but it also has a general obligation to comply with the law. An instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.
的確，受託運用者有義務遵守控管者的指令，但亦有遵守法律的一般義務。違反資料保護法的指令似乎會導致上述二項義務之間的衝突。

148. Once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually violates data protection law.
一旦獲知其指令之一可能違反資料保護法，控管者必須評估狀況並查明該指令是否確實違反資料保護法。

149. The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context. One

example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction. Another example would be a clause on the possibility for the processor to suspend the implementation of the affected instruction until the controller confirms, amends or withdraws its instruction.[68]
EDPB 建議雙方協商並在合約中商定受託運用者發出侵權指令通知，以及在此情況下控管者不採取行動的結果。一種做法是，增加一條如果控管者堅持非法指令，就終止合約的條款。另一個案例是受託運用者暫停執行受影響指示之可能性的條款，直到控管者確認、修改或撤回其指示。

1.5Processor determining purposes and means of processing
1.5受託運用者決定運用的目的和方法

150. If the processor infringes the Regulation by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR).
如果受託運用者因決定運用的目的和方式而違反了規則，則應將其視為該運用的控管者（GDPR 第 28(10)條）。

1.6Sub-processors
1.6次受託人

151. Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data. The analysis of whether the service provider acts as a sub-processor should be carried out in line with what described above on the concept of processor (see above paragraph 83).
資料運用活動通常由大量參與者執行，系列分包變得越來越複雜。GDPR 引入特定義務，當受託運用者打算委託另一人時就啟動這些義務，因而透過將所需的個人資料運用活動之委託，以在這系列中加入另一個連結。對服務提供者是否作為次受託人之分析應依照上述對受託運用者概念之描述(參見上文第 83 段)。

---

[68] See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 39.
見 EDPB -歐盟資料保護監督機關 1/2021 就控管者與受託運用者標準合約條款的共同意見，第 39 段。

152. Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor[69].
雖然，這個系列可能很長，但控管者仍居於決定運用目的和方式的關鍵角色。GDPR 第 28(2)條規定，未經控管者事先以書面特定或概括授權，受託運用者不得委託其他受託運用者。在概括的書面授權時，受託運用者必須將有關增加或更換其他受託運用者的任何更改計畫通知控管者，使控管者有機會對這些改變表示異議。在這兩種情況下，受託運用者將任何個人資料運用委託給次受託人之前，應獲得控管者的書面授權。為了進行評估並決定是否授權複委託，受託運用者必須提供資料控管者一份打算複委託的次受託人名單（包括各個次受託人的所在地、運作內容及已實施哪些保護措施的證明）。

153. The prior written authorisation may be specific, i.e. referring to a specific sub-processor for a specific processing activity and at a specific time, or general. This should be specified in the contract or other legal act that governs the processing.
事先書面授權可以是特定的，亦即針對在特定時間和特定運用活動有關的特定次受託人，也可以是概括性的。這應在合約或其他規範資料運用的法律文件中明定。

154. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.

---

[69] This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.
這份資料是必要的，如此，控管者才能遵守 GDPR 第 24 條課責性原則和第 28(1)及 32 條和第五章規定。

控管者在簽署合約時決定接受某些次受託人時，經核准的次受託人名單應作為合約附件。之後，名單應依據控管者給予的概括或特定授權隨時更新。

155. If the controller chooses to give its **specific authorisation**, it should specify in writing which subprocessor and what processing activity it refers to. Any subsequent change will need to be further authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees" (see section 1.1 above[70]).
如果，控管者選擇給予特定授權，應以書面特定其所指的是哪個次受託人和哪些資料運用。任何後續變動都需得到控管者的進一步授權才能實施。如果受託運用者請求的特定授權沒有在預定期間內得到回覆，即應視為拒絕授權。控管者同意或拒絕授權時，應考慮其有義務僅使用提供「充分保證」之受託運用者（參見上文第 1.1 節）。

156. Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources)[71]. In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object.
或者，控管者可以概括授權使用次受託人（在合約附件中包含次受託人名單），但應訂定受託運用者選擇次受託人的標準作為補充指引（例如，在技術上和組織上措施的保證、專業知識、可靠性和資源）。在此情況下，受託運用者必須在適當時候通知控管者任何增加或更換次受託人的計畫，以便給控管者有表示異議的機會。

157. Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the meaning given to the controller's silence: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.

---

[70] See Part II - sub-section 1.1 ("Choice of the processor").
見第二部分第 1.1 節（「受託運用者的選擇」）。

[71] This duty of the controller stems from the accountability principle in Article 24 and from the obligation to comply with provisions of Articles 28(1), 32 and Chapter V of the GDPR.
控管者的這項職責來自 GDPR 第 24 條課責性原則和遵守第 28(1)及 32 條和第五章的義務。

因此，特定授權和概括授權情況的主要區別在於控管者的沉默所代表的含義：在概括授權的情況下，控管者在預定期間內未表示異議，可以解釋為同意授權。

158. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic (e.g. templates). Such timeframe needs to be reasonable in light of the type of processing, the complexity of the activities entrusted to the processor (and the sub-processors) and the relationship between the parties. In addition, the contract should include details as to the practical steps following the controller's objection (e.g. by specifying time frame within which the controller and processor should decide whether the processing shall be terminated).
在這兩種情況下，合約都應詳細說明給控管者同意或反對的期間，以及雙方打算如何就這個議題進行溝通（例如範本）。合理期間應考量資料運用型態、委託給受託運用者（以及次受託人）的活動複雜度，以及各方之間的關係。此外，合約應包含控管者異議後的實際步驟之細節（例如：指定控管者和受託運用者應決定是否終止運用的時間範圍）。

159. Regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR). Therefore, the processor should ensure it proposes sub-processors providing sufficient guarantees.
無論控管者建議選擇供應商的標準為何，受託運用者應為次受託人義務的履行，對控管者負全部責任（GDPR 第 28(4)條）。因此，受託運用者應確保其提議的次受託人提供足夠的保證。

160. Furthermore, when a processor intends to employ an (authorised) sub-processor, it must enter into a contract with it that imposes the same obligations as those imposed on the first processor by the controller or the obligations must be imposed by another legal act under EU or Member State law. The whole chain of processing activities needs to be regulated by written agreements. Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty. As an example, as to assistance with data breach related obligations, notification of a data breach by a sub-processor directly to the controller could be done if all three agree. However, in the case of such direct

notification the processor should be informed and get a copy of the notification.
此外，當受託運用者打算委託（授權的）次受託人時，必須與其簽訂合約，課予控管者對第一個受託運用者加諸的相同義務，或由另一份依據歐盟或成員國法律而定的法律文件課予義務。資料運用的整串活動，必須受到書面合約的規範。施加「相同」義務應以功能而非形式解釋：合約不必包含與控管者和受託運用者的合約中所使用完全相同的字句，但應確保實質上的義務相同。這也表示，如果受託運用者將資料運用的特定部分複委託給次受託人，而某些義務不適用於此，則此類義務不應「內定」包含在與次受託人的合約中，因為這只會產生不確定性。例如，為了協助履行與個資外洩相關的義務，如果三方都同意，則可以由次受委託人直接向控管者通知個資外洩。但是，於此直接通知的情況，應通知受託運用者並提供通知的副本。

2 CONSEQUENCES OF JOINT CONTROLLERSHIP
2 共同控管的結果

2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR
2.1 以透明方法確定共同控管者遵守 GDPR 義務的個別責任

161. Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation.
GDPR 第 26(1)條規定，共同控管者應以透明方式確定並就各自遵守本規則義務的責任達成合意。

162. Joint controllers thus need to set “who does what” by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term “*respective*” in Article 26(1). This does not preclude that EU or Member State law may already set out certain responsibilities of each joint controller. Where this is the case, the joint controller arrangement should also address any additional responsibilities necessary to ensure compliance with the GDPR that are not addressed by the legal provision.[72]

[72] "In any event, the joint controller arrangement should comprehensively address all of the responsibilities of the joint controllers, including those which may have already been set out in the relevant EU or Member State law and without prejudice to the obligation of joint controllers to make available the essence of the joint controller arrangement in accordance with Article 26(2) GDPR."
「無論如何，共同控管者的安排應全面處理共同控管者的所有責任，包括可能已在相關歐盟或成員國法律中規定的責任，並且不影響共同控管者依據 GDPR 第 26(2)條規定針對共同控管者安排的重點

因此，共同控管者需要透過決定他們之中誰必須執行哪些任務來設定「誰做什麼」，以確保資料運用符合 GDPR 中與所討論的共同運用有關的相關義務。換言之，應依據第 26(1)條中「各自」一詞來分配合規責任。但這不排除歐盟或成員國法律可能已經規定了每個共同控管者的某些責任。如果有這種情況，共同控管者的安排還必須包括法律沒有規定但為確保遵守 GDPR 所必需之額外責任。

163. The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement. The EDPB observes that there are situations occurring in which the influence of one joint controller and its factual influence complicate the achievement of an agreement. However, those circumstances do not negate the joint controllership and cannot serve to exempt either party from its obligations under the GDPR.
這些規則的目的是確保在涉及多個參與者，尤其是在複雜的資料運用環境中時，明確分配遵守資料保護規則的責任，以避免對個人資料的保護降低，或負面的權限衝突導致漏洞，因而，使參與運用過程的任何一方不遵守某些義務。在此應說清楚，所有的責任都必須依據實際情況加以分配，才能達成操作合約。EDPB 觀察到，某些情況下，一個共同控管者的影響及其事實影響會使合約之達成變得複雜。然而，這些情況並不否定共同控管的情形，也不能免除任何一方依 GDPR 之義務。

164. More specifically, Article 26(1) specifies that the determination of their respective responsibilities (i.e. tasks) for compliance with the obligations under the GDPR is to be carried out by joint controllers "*in particular"* as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.
更確切地說，第 26(1)條明確規定他們各自遵守 GDPR 規定義務的責任（即任務），將由共同控管者執行，「特別是」第 13 和第 14 條提到關於當事人行使權利和提供訊息的責任，除非而且是控管者各自的責任由歐盟或控管者所在成員國的法律所明定。

課予的義務。」

165. It is clear from this provision that joint controllers need to define who respectively will be in charge of answering to requests when data subjects exercise their rights granted by the GDPR and of providing information to them as required by Articles 13 and 14 of the GDPR. However, the use of the terms "*in particular*" indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller's obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.
從這條規定可以清楚看出，當事人行使 GDPR 權利時，共同控管者需要界定分別由誰負責回應當事人請求，並按照 GDPR 第 13 和 14 條規定提供資訊給當事人。然而，使用「特別是」的用語顯示，本條規定並未窮盡參與各方遵守責任分配的義務。共同控管者的合規責任分配不僅限於第 26(1)條提到的議題，還延伸到依據 GDPR 規定的其他控管者的義務。共同控管者確實需要確保整個共同運用資料的活動完全符合 GDPR 規定。

166. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:
從這個角度來看，除了第 26(1)條明定的內容外，共同控管者在確定各自責任時，應考慮的合規措施和相關義務包括但不限於：

- Implementation of general data protection principles (Article 5)
  採行一般資料保護原則（第 5 條）
- Legal basis of the processing[73] (Article 6)
  資料運用的法定事由（第 6 條）
- Security measures (Article 32)
  安全措施（第 32 條）
- Notification of a personal data breach to the supervisory authority and to the data subject[74](Articles 33 and 34)

[73] Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.
雖然 GDPR 並未禁止共同控管者依據不同的法定事由運用資料，仍建議，只要可能的話，就特定目的仍採用相同的法定事由。

[74] Please also see EDPB guidelines on Personal data breach notification under Regulation 2016/679, WP250.rev.01 which provide that joint controllership will include "*determining which party will have*

將個人資料侵害事件通報監管機關和當事人（第 33 和 34 條）

- Data Protection Impact Assessments (Articles 35 and 36)[75]
  資料保護影響評估（第 35 和 36 條）
- The use of a processor (Article 28)
  受託運用者之採用（第 28 條）
- Transfers of data to third countries (Chapter V)
  將資料傳輸到第三個（第五章）
- Organisation of contact with data subjects and supervisory authorities
  聯絡當事人和監管機關的組織

167. Other topics that could be considered depending on the processing at stake and the intention of the parties are for instance the limitations on the use of personal data for another purpose by one of the joint controllers. In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing. Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.[76]
依據所討論的運用和參與運用各方的意圖，可以考慮的其他主題是，例如，對共同控管者之一將個人資料用於其他目的的限制。在這方面，

---

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"(p.13).
另見 EDPB 依規則對個人資料侵害通知之 2016/679 第 WP250 號指引修訂一版，規定共同控管包括「確定何方有責任遵守第 33 和 34 條的義務。第 WP29 號指引建議共同控管者間的合約包含確定哪個控管者將率先或負責遵守 GDPR 的侵害通知義務」（13 頁）。

75 Please also see EDPB guidelines on DPIAs, WP248.rev01 which provide the following: "*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*" (p.7).
另見 EDPB 對 DPIAs 第 WP248 號指引修訂一版，規定如下：「當資料運用涉及共同控管者，他們需精確定義各自義務。他們的個資保護影響評估應訂定誰負責處理資料運用風險和保護當事人權利與自由的各種措施。每個資料控管者應表達各自需求，並在不透露機密（例如保護營業秘密、智慧財產、機密商業資訊）或揭露弱點的情況下分享有用資訊」（第七頁）。

76 Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller. In other words, the existence of a joint controller relationship does not automatically mean that the joint controller receiving the data can also lawfully process the data for additional purposes which are beyond the scope of joint control.
無論接收方是另一個控管者或共同控管者，控管者的揭露須有法律依據與妥適性評估。換言之，共同控管關係的存在不當然表示收到資料的共同控管者也可以為了逾越共同控管範圍以外的目的而合法運用資料。

二位控管者永遠有責任確保他們都有運用資料的法律依據。有時，在共同控管的情況下，個人資料由一個控管者分享給另一個控管者。基於課責性，每個控管者都有責任確保資料不會以與共享資料的控管者最初蒐集目的不相容的方式進一步運用。

168. Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle.
共同控管者只要確保資料運用完全符合 GDPR 規定，在分配彼此義務時享有一定程度的彈性。分配應考慮誰有能力並能有效確保當事人權利，遵守 GDPR 規定的相關義務等因素。EDPB 建議記錄相關因素和內部分析，以便分配不同的義務。這種分析是課責性原則下文件的一部分。

169. The obligations do not need to be equally distributed among the joint controllers. In this respect, the CJEU has recently stated that "*the existence of joint* responsibility *does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*"[77]. However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools.
義務不需要在所有共同控管人間平均分配。在這方面，歐盟法院最近表示，「共同責任的存在不一定表示參與個人資料運用的各個操作者責任相同」。然而，考慮到共同運用資料的性質和脈絡，可能發生並非所有義務都可以分配的情況，而且每一個共同控管者可能都需要遵守 GDPR 的相同規定。例如，共同控管者使用共享資料運用工具或系統，需要確保特別遵守目的限制原則，並採取適當措施確保在共享工具下運用的個人資料安全性。

[77] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 43.
「*Wirtschaftsakademie*」案判決，C-210/16, ECLI:EU:C:2018:388，第 43 段。

170. Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers.
另一個案例是，如果符合第 37(1)條的條件，每個共同控管者必須保存運用活動的紀錄或指定一名資料保護長(DPO)。這樣的要求與共同運用無關，但適用於控管者。

2.2 Allocation of responsibilities needs to be done by way of an arrangement
2.2 責任分配需要透過安排

2.2.1 Form of the arrangement
2.2.1 安排的形式

171. Article 26(1) of the GDPR provides as a new obligation for joint controllers that they should determine their respective responsibilities "*by means of an arrangement between them*". The legal form of such arrangement is not specified by the GDPR. Therefore, joint controllers are free to agree on the form of the arrangement.
GDPR 第 26(1)條提出共同控管者的一個新義務，他們應「藉由他們之間的安排」確定各自的責任。GDPR 並未明定此類安排的法律形式。因此，共同控管者可以自由約定安排的形式。

172. In addition, the arrangement on the allocation of responsibilities is binding upon each of the joint controllers. They each agree and commit *vis-à-vis* each other on being responsible for complying with the respective obligations stated in their arrangement as their responsibility.
此外，責任分配的安排對每個共同控管者都有約束力。他們每個人都同意並彼此承諾有責任遵守其安排中課予他們的各自義務。

173. Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR.

因此，基於法律明確性原則，即使 GDPR 沒有對合約或其他法律文件的法律要求，EDPB 也建議以具有約束力的文件做出此類安排，例如合約或其他依歐盟或控管者所在成員國法律規定具有法律約束力的文件。這將帶來明確性，並可用於證明透明度和課責性。確實，如果有一方不遵守大家同意的責任義務分配，文件的約束性容許一個控管者就合約中規定屬於另一方的責任範圍追究其責任。此外，依據課責性，使用合約或其他法律文件讓共同控管者可以證明他們遵守 GDPR 課予的義務。

174. The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement[78]. This requirement is important as it ensures legal certainty and avoid possible conflicts not only in the relation between the joint controllers but also visà-vis the data subjects and the data protection authorities.
責任（即任務）在每個共同控管者之間的分配方式必須以清晰明瞭的語言陳述。這個要求很重要，因為它確保法律明確性，並避免了共同控管者之間、當事人和資料保護機關關係中的可能衝突。

175. To better frame the allocation of responsibilities between the parties, the EDPB recommends that the arrangement also provide general information on the joint processing by notably specifying the subject matter and purpose of the processing, the type of personal data, and the categories of data subjects.
為了更明確界定各方的責任分配，EDPB 建議該安排也透過清楚說明資料運用的主題和目的、個人資料類型和當事人類別，提供有關共同運用的一般資訊。

2.2.2. Obligations towards data subjects
2.2.2 對當事人的義務

176. The GDPR provides several obligations of joint controllers towards data subjects:
GDPR 規定數項共同控管者對當事人的義務：

The arrangement shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects
安排應充分反映共同控管者各自相對於當事人的角色和關係

[78] As stated in recital 79 of the GDPR *"(...) the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers*".
如 GDPR 前言第 79 段所述，「控管者與受託運用者的責任和義務，還有監管機關的監管和措施，需要明確分配本規則所定的責任，包括控管者和其他控管者共同確定資料運用目的和方式的情況」。

177. As a complement to what is explained above in section 2.1 of the present guidelines, it is important that the joint controllers clarify in the arrangement their respective role, "*in particular*" as regards the exercise of the rights of the data subject and their duties to provide the information referred to in Articles 13 and 14. Article 26 of the GDPR stresses the importance of these specific obligations. The joint controllers must therefore organise and agree on how and by whom the information will be provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3) as further explained below.
作為對本指引第 2.1 節解釋的補充，重要的是共同控管者在安排中闡明各自角色，「特別是」在當事人行使權利及提供第 13 和第 14 條所提資料的義務。GDPR 第 26 條強調這些特定義務的重要性。因此，共同控管者必須安排並商定如何以及由誰提供資料，還有如何以及由誰回覆當事人請求。無論關於這一點的安排內容為何，當事人都可以依據第 26(3)條規定，聯絡任一位共同控管者行使他們的權利，說明如下。

178. The way these obligations are organised in the arrangement should "*duly*", i.e. accurately, reflect the reality of the underlying joint processing. For example, if only one of the joint controllers communicates with the data subjects for the purpose of the joint processing, such controller could be in a better position to inform the data subjects and possibly to answer their requests.
這些義務在安排中的組織方式應「適當地」，亦即準確地反映潛在共同運用的實際情況。例如，如果只有一個共同控管者為了共同運用的目的與當事人通訊，則該控管者將更有能力通知當事人並可能回覆他們的請求。

The essence of the arrangement shall be made available to the data subject
安排的重點應讓當事人知悉

179. This provision is aimed to ensure that the data subject is aware of the "*essence of the arrangement*". For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller). The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what.
本條旨在確保當事人了解「安排的本質」。例如，當事人必須完全清楚哪個控管者是當事人行使權利的聯絡人（儘管他們可以行使有關和對

抗每個共同控管者的權利）。在共同控管的情況下，讓當事人得知安排重點的義務很重要，以便當事人知道哪個控管者負責什麼。

180. What should be covered by the notion of "*essence of the arrangement*" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject, and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated.
GDPR 沒有具體說明「安排的本質」概念應涵蓋的內容。EDPB 建議其本質至少應涵蓋第 13 和 14 條中所提當事人已經可以存取的資料的所有要素，而且就這每一個要素而言，安排應明確說明哪個共同控管者負責確保符合這些要素。安排的重點也必須指明聯絡人（如果有指定）。

181. The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "*upon request*" nor "*publicly available by way of appropriate means*". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner.
讓當事人獲知這類資訊的方式沒有特定。與 GDPR 其他條款（例如，關於資料運用紀錄的第 30(4)條或關於登記經核准的行為準則的第 40(11)條）相反，第 26 條並未表明可用性應「依據請求」或「經由適當方式公開取得」。因此，由共同控管者決定將安排重點讓當事人知悉的最有效方式（例如，連同第 13 或 14 條的資訊、寫在隱私政策，依據資料保護長的要求（若有），或提供給可能已指定的聯絡人）。共同控管者應分別確保以一致方式提供資料。

The arrangement may designate a contact point for data subjects
該安排可以為當事人指定聯絡人

182. Article 26(1) provides the possibility for joint controllers to designate in the arrangement a contact point for data subjects. Such designation is not mandatory.
第 26(1)條規定，共同控管者可以在安排中指定當事人的聯絡人。這種指定不具強制性。

183. Being informed of a single way to contact possible multiple joint controllers enables data subjects to know who they can contact with regard to all issues related to the processing of their personal data. In addition, it allows multiple joint controllers to coordinate in a more efficient manner their relations and communications *vis-à-vis* data subjects.
獲知與可能有多個共同控管者聯絡的單一方式，使當事人能夠知道他們可以就與其個人資料運用相關的所有問題聯絡誰。此外，它讓多個共同控管者以更有效的方式協調他們與當事人的關係和通訊。

184. For these reasons, in order to facilitate the exercise of data subjects' rights under the GDPR, the EDPB recommends joint controllers to designate such contact point.
出於這些原因，為了促進當事人行使 GDPR 規定的權利，EDPB 建議共同控管者指定聯絡人。

185. The contact point can be the DPO, if any, the representative in the Union (for joint controllers not established in the Union) or any other contact point where information can be obtained.
聯絡人可以是個資保護長（如果有）、歐盟代表（對於未設立在歐盟的共同控管人）或任何其他可以獲得資料的聯絡人。

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.
無論安排的條款如何，當事人都可以行使有關和對抗每個共同控管者的權利。

186. Under Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.
依據第 26(3)條，當事人不受安排條款約束，且可以依據 GDPR 行使有關和對抗每個共同控管者的權利。

187. For example, in case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.
例如，控管者設立在不同成員國，或只有其中一名控管者設立在歐盟時，當事人可以自行選擇聯絡他們居住或工作地所在成員國設立的控管者，或設立在歐盟其他地方或歐洲經濟區的控管者。

188. Even if the arrangement and the available essence of it indicate a contact point to receive and handle all data subjects' requests, the data subjects themselves may still choose otherwise.
即使安排並可實質指明一個聯絡人受理和處理所有當事人的請求，當事人仍然可以選擇其他人。

189. Therefore, it is important that joint controllers organise in advance in their arrangement how they will manage answers to requests they could receive from data subjects. In this respect, it is recommended that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled. Requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights under the GDPR.
因此，重要的是，共同控管者在安排中事先規畫他們如何回覆當事人的請求。關於這一點，建議共同控管者將收到的請求傳給其他負責的控管者或指定聯絡人，以便有效處理。要求當事人聯絡指定的聯絡人或負責的控管者，會給當事人帶來過多負擔，違背 GDPR 促進當事人行使權利的宗旨。

2.3Obligations towards data protection authorities
2.3對資料保護機關的義務

190. Joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer.
共同控管者應在安排中規定他們與資料保護監管機關溝通的方式。此類溝通包括依據 GDPR 第 36 條規定的可能諮詢、個人資料侵害通知、資料保護長的指定。

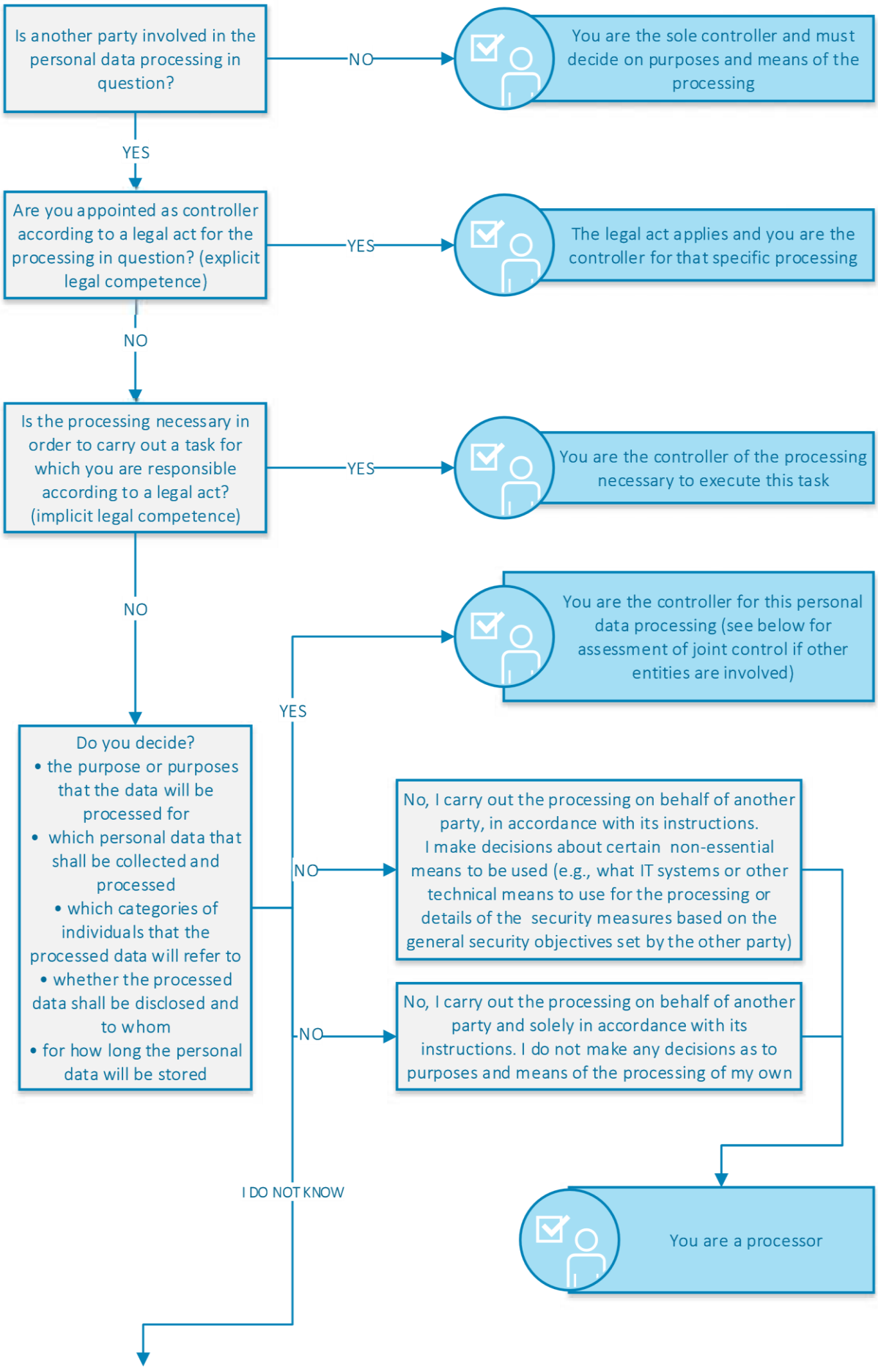
191. It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing.
應該記得的是，資料保護機關不受安排條款所約束，無論是在各方作為共同控管人的資格問題或指定聯絡人的問題。因此，當局可以聯絡任何共同控管者，行使其依第 58 條關於資料共同運用規定的職權。

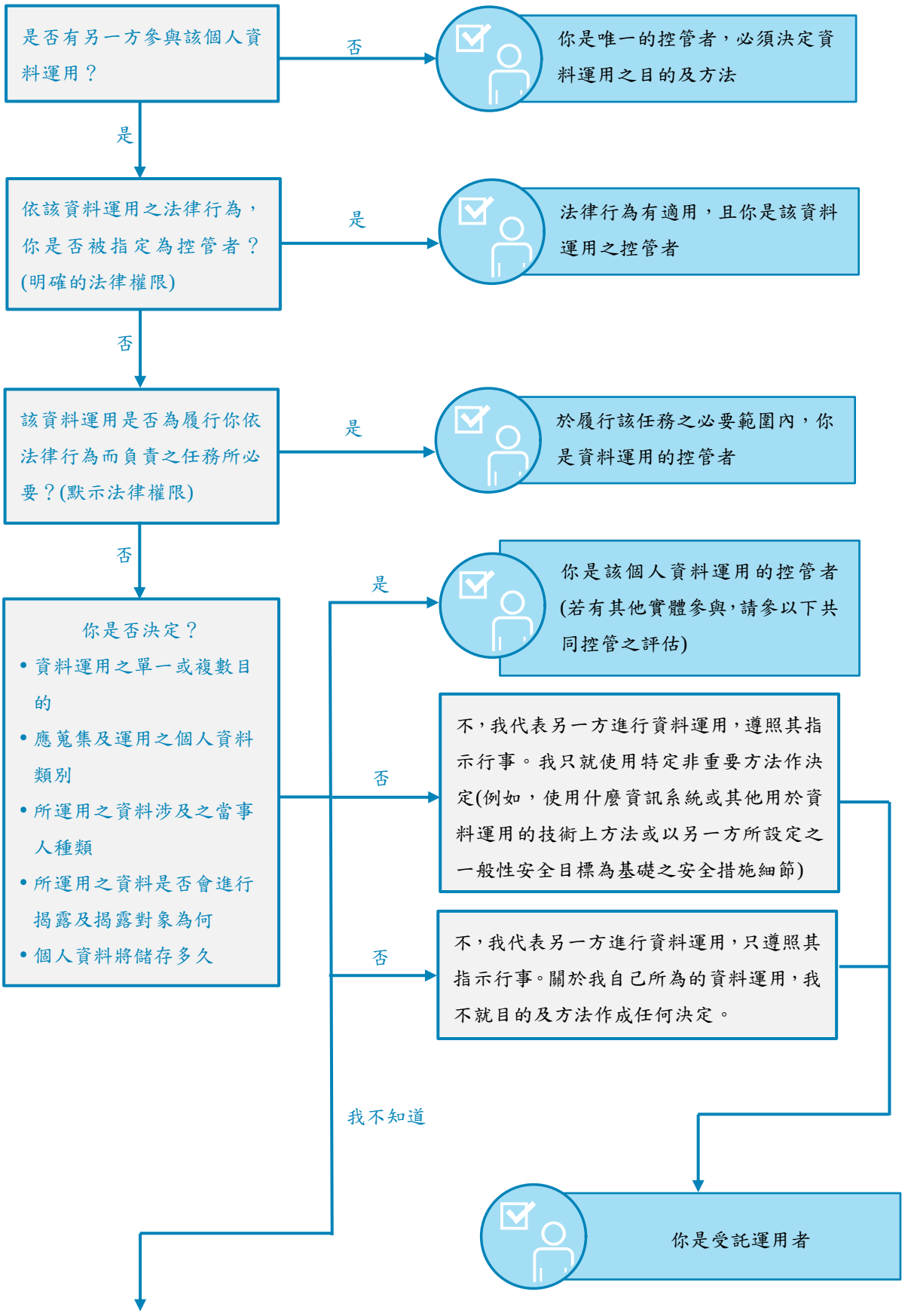
Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

附錄 I–控管者、受託運用者及共同控管者概念之應用流程圖

Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.

註：為妥適評估每個參與實體的角色，必須先確認所討論的個人資料運用過程及其確切目的。如果有多個實體參與，必須評估目的及方式是否共同決定進而產生共同控管。


Is another party involved in the personal data processing in question?
NO
You are the sole controller and must decide on purposes and means of the processing
YES
Are you appointed as controller according to a legal act for the processing in question? (explicit legal competence)
YES
The legal act applies and you are the controller for that specific processing
NO
Is the processing necessary in order to carry out a task for which you are responsible according to a legal act? (implicit legal competence)
YES
You are the controller of the processing necessary to execute this task
NO
You are the controller for this personal data processing (see below for assessment of joint control if other entities are involved)
YES
Do you decide?
• the purpose or purposes that the data will be processed for
• which personal data that shall be collected and processed
• which categories of individuals that the processed data will refer to
• whether the processed data shall be disclosed and to whom
• for how long the personal data will be stored
NO
No, I carry out the processing on behalf of another party, in accordance with its instructions. I make decisions about certain non-essential means to be used (e.g., what IT systems or other technical means to use for the processing or details of the security measures based on the general security objectives set by the other party)
NO
No, I carry out the processing on behalf of another party and solely in accordance with its instructions. I do not make any decisions as to purposes and means of the processing of my own
I DO NOT KNOW
You are a processor


是否有另一方參與該個人資料運用？
否
你是唯一的控管者，必須決定資料運用之目的及方法
是
依該資料運用之法律行為，你是否被指定為控管者？(明確的法律權限)
是
法律行為有適用，且你是該資料運用之控管者
否
該資料運用是否為履行你依法律行為而負責之任務所必要？(默示法律權限)
是
於履行該任務之必要範圍內，你是資料運用的控管者
否
你是否決定？
• 資料運用之單一或複數目的
• 應蒐集及運用之個人資料類別
• 所運用之資料涉及之當事人種類
• 所運用之資料是否會進行揭露及揭露對象為何
• 個人資料將儲存多久
是
你是該個人資料運用的控管者(若有其他實體參與，請參以下共同控管之評估)
否
不，我代表另一方進行資料運用，遵照其指示行事。我只就使用特定非重要方法作決定(例如，使用什麼資訊系統或其他用於資料運用的技術上方法或以另一方所設定之一般性安全目標為基礎之安全措施細節)
否
不，我代表另一方進行資料運用，只遵照其指示行事。關於我自己所為的資料運用，我不就目的及方法作成任何決定。
我不知道
你是受託運用者

I DO NOT KNOW

I don't know who decides on the purposes or means of the processing. :

The following factors may help to determine the appropriate qualification of the roles:

Factors that indicate that you are the controller

- You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller)
- You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees)
- The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view
- The processing refers to your relation with the data subjects as employees, customers, members etc.
- You have complete autonomy in deciding how the personal data is processed
- You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf

Factors that indicate that you are the processor

- You process the personal data for another party's purposes and in accordance with its documented instructions - you do not have a purpose of your own for the processing.
- Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract.
- You do not pursue your own purpose in the processing other than your own business interest to provide services.
- You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions (you are a sub-processor)

我不知道

我不知道資料運用之目的或方法是由誰決定

下列因素可能有助於決定如何進行角色區別較為適當：

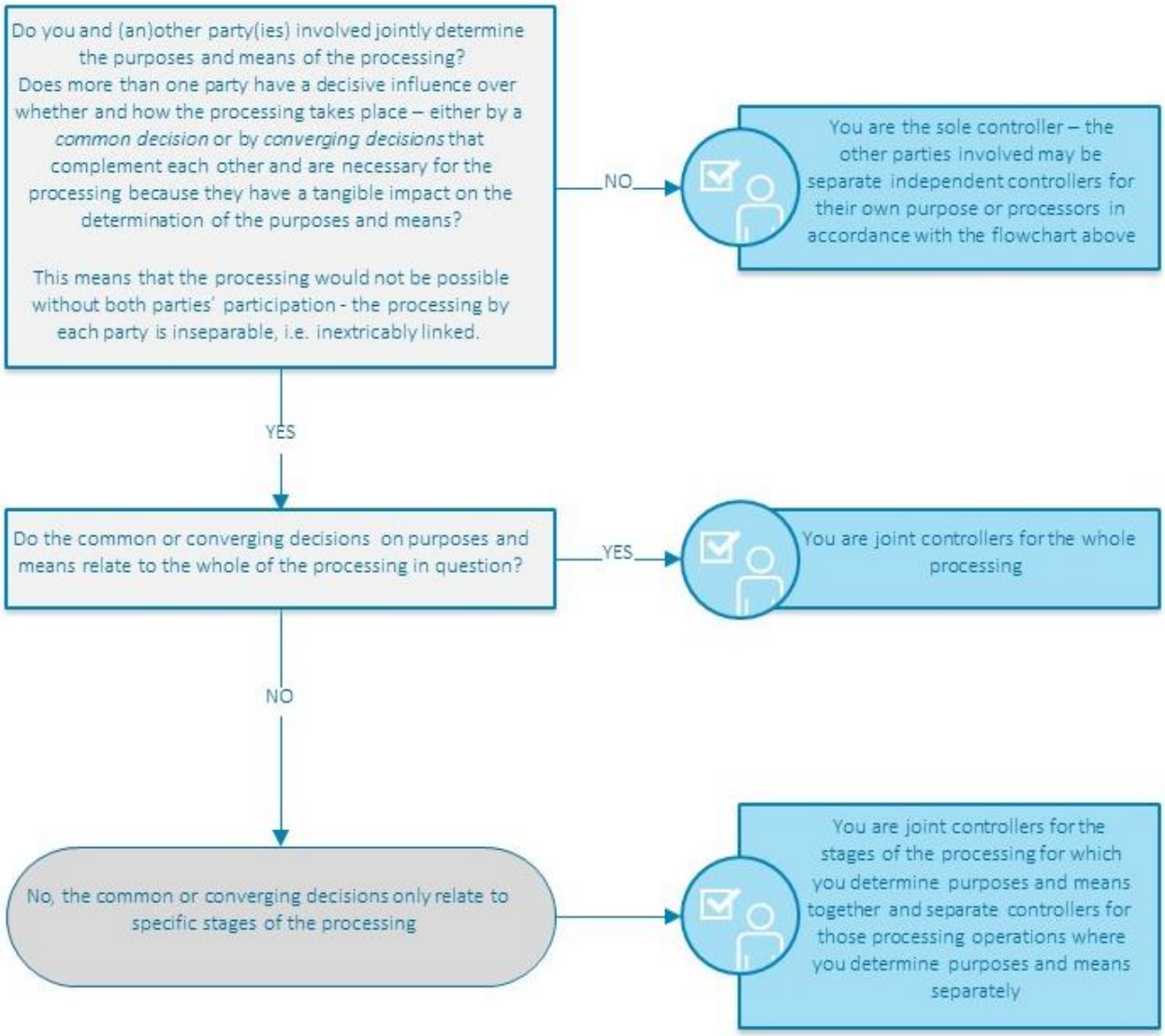
表徵你是控管者的因素

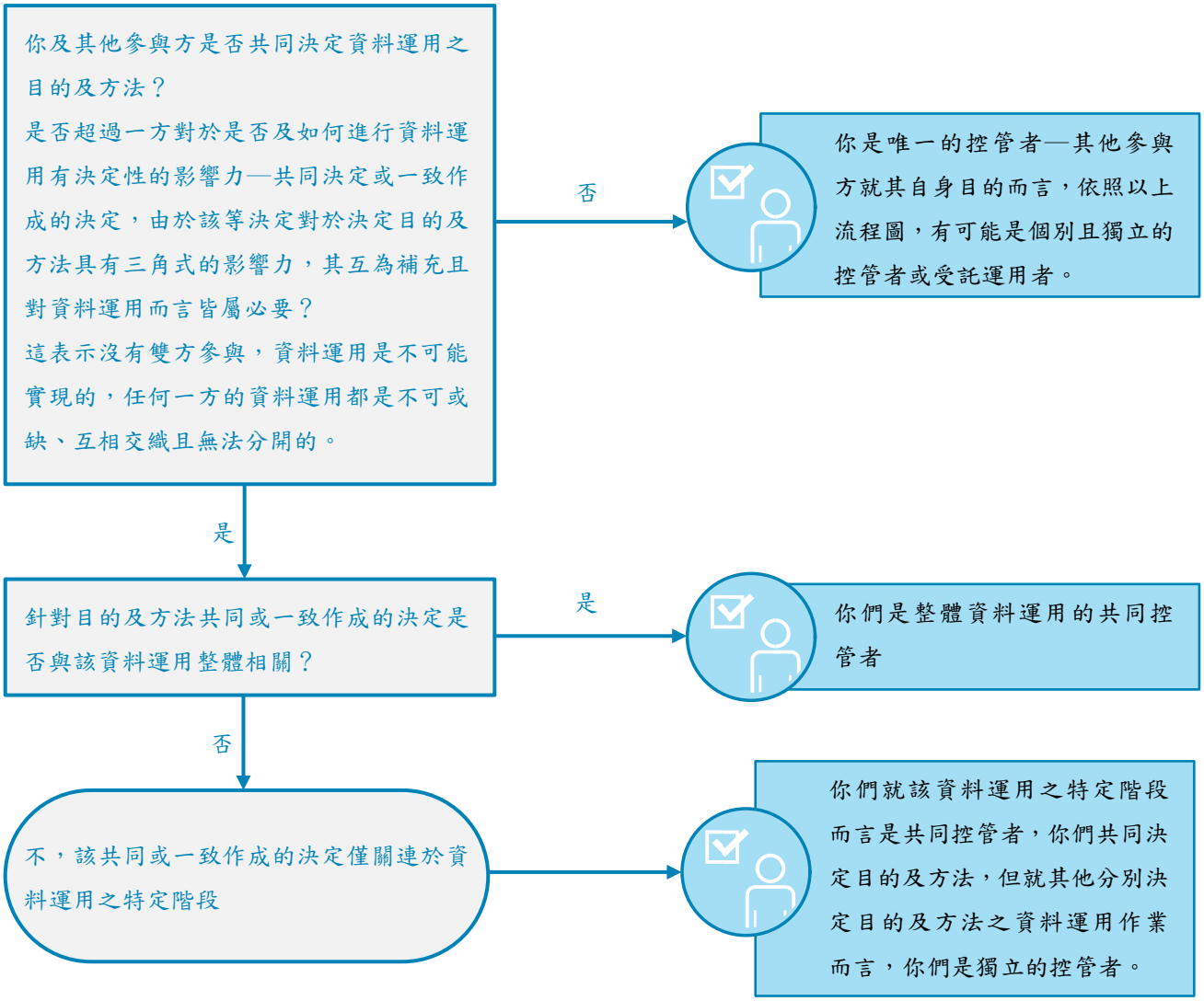
- 你因資料運用而獲益(或擁有利益)(僅因提供服務而從其他控管者收受款項者除外)
- 你針對相關個人所作成的決定為資料運用之一部分或結果(例如，當事人是你的員工)
- 資料運用活動自然地依附於你的角色或活動(例如，由於傳統角色或專業技能)，從資料保護觀點看來，該等角色或活動必須承擔責任
- 資料運用涉及你與當事人(作為員工、顧客、會員等)之間的關係
- 決定如何運用個人資料時，你擁有完全的自主性
- 你已將個人資料運用委託給外部組織，由其代表你運用該個人資料

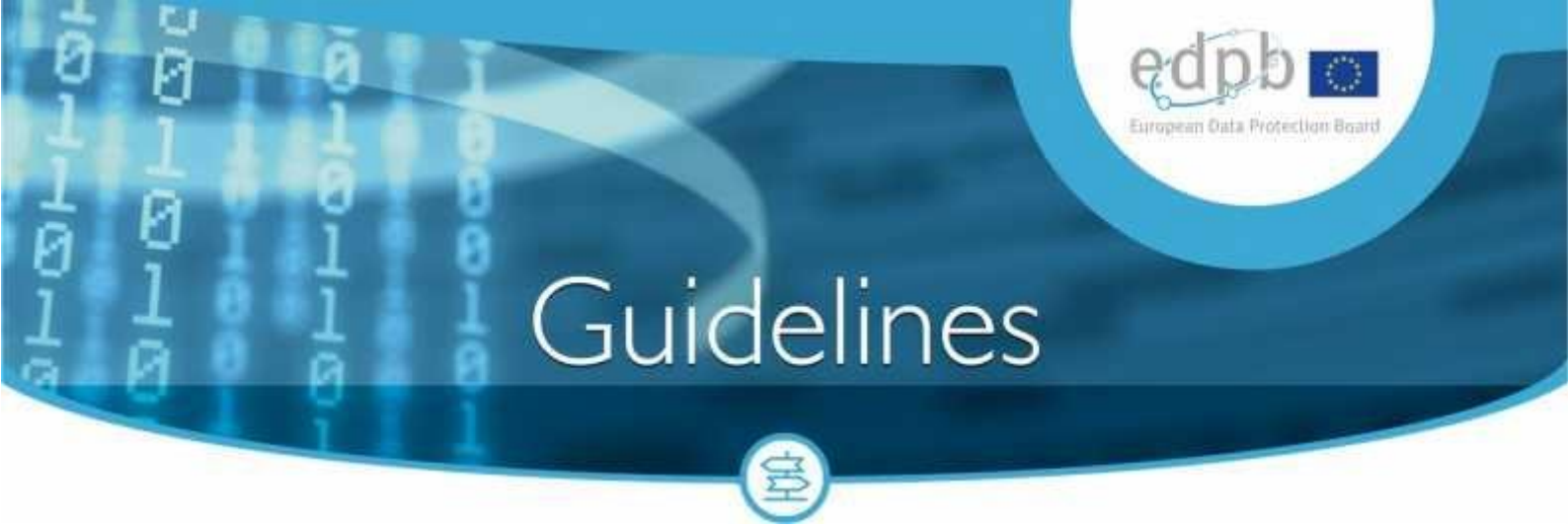
表徵你是受託運用者的因素

- 你為其他方之目的運用該個人資料，並遵照其文件化指示—你對於自身所進行的資料運用並沒有任何目的。
- 其他方監督你的資料運用活動，以確保你遵照指示及契約條款。
- 除了提供服務之自身商業利益外，你運用資料時並未追求自身之目的。
- 你受他人委託執行特定資料運用活動，該他人則受其他方委託代表其他方運用資料，並遵照其他方文件化指示(你是次受託人)

Joint controllership - If you are the controller and other parties are involved in the personal data processing:
共同控管—如果你是控管者且有其他方參與個人資料運用：




你及其他參與方是否共同決定資料運用之目的及方法？
是否超過一方對於是否及如何進行資料運用有決定性的影響力—共同決定或一致作成的決定，由於該等決定對於決定目的及方法具有三角式的影響力，其互為補充且對資料運用而言皆屬必要？
這表示沒有雙方參與，資料運用是不可能實現的，任何一方的資料運用都是不可或缺、互相交織且無法分開的。
否
你是唯一的控管者—其他參與方就其自身目的而言，依照以上流程圖，有可能是個別且獨立的控管者或受託運用者。
是
針對目的及方法共同或一致作成的決定是否與該資料運用整體相關？
是
你們是整體資料運用的共同控管者
否
不，該共同或一致作成的決定僅關連於資料運用之特定階段
你們就該資料運用之特定階段而言是共同控管者，你們共同決定目的及方法，但就其他分別決定目的及方法之資料運用作業而言，你們是獨立的控管者。



Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR
一般資料保護規則（GDPR）對於被遺忘權於搜尋引擎案例適用標準之指引 5/2019

(part 1)
（第一部分）

Adopted on 7 July 2020
2020 年 7 月 7 日通過

Version 2.0
版本 2.0

Version history
版本歷程

Version 2.0 2.0 版	2020 年 7 月 7 日	Adoption of the Guidelines after public consultation 經徵詢公眾意見後通過本指引
Version 1.1 1.1 版	2020 年 2 月 17 日	Minor corrections 微幅調整
Version 1.0 1.0 版	2019 年 12 月 2 日	Adoption of the Guidelines for public consultation 徵詢公眾意見通過本指引

Table of contents
目錄

INTRODUCTION 導言 4

1. THE GROUNDS OF THE RIGHT TO REQUEST DELISTING UNDER GDPR
根據 GDPR 行使去列表權之事由 9

1.1 Ground 1: The Right to request delisting when the personal data are no longer necessary in relation to the search engine provider's processing (Article 17.1.a)
事由 1：個人資料對於搜尋引擎之運用活動已經沒有必要而行使去列表權（第 17.1.a 條） 10

1.2 Ground 2: The Right to request delisting when the data subject withdraws consent where the legal basis for the processing is pursuant to Article 6.1.a or Article 9.2.a GDPR and where there is no other legal basis for the processing (Article 17.1.b)
事由 2：運用行為係依據 GDPR 第 6.1.a 或 9.2.a 條規定之當事人同意，且無其他法定事由，當事人因撤回同意而行使去列表權（第 17.1.b 條） .. 12

1.3 Ground 3: The Right to request delisting when the data subject has exercised his or her Right to object to the processing of his or her personal data (Article 17.1.c)
事由 3：當事人行使拒絕運用其個人資料之權利而行使去列表權（第 17.1.c 條） 13

1.4 Ground 4: The Right to request delisting when the personal data have been unlawfully processed (Article 17.1.d) 事由 4：個人資料遭違法運用而行使去列表權（第 17.1.d 條） 16

1.5 Ground 5: The Right to request delisting when the personal data have to be erased for compliance with a legal obligation (Article 17.1.e) 事由 5：為遵守法定義務而有必要刪除個人資料之去列表權（第 17.1.e 條） 17

1.6 Ground 6: The Right to request delisting when the personal data have been collected in relation to the offer of information society services (ISS) to a child (Article 17.1.f) 事由 6：個人資料之蒐集與提供「資訊社會服務」（ISS）給兒童有關而行使去列表權（第 17.1.f 條） 18

2. THE EXCEPTIONS TO THE RIGHT TO REQUEST DELISTING UNDER ARTICLE 17.3 依據第 17.3 條規定行使去列表權之例外 19

2.1 Processing is necessary for exercising the right of freedom of expression and information 資料運用係行使表意與資訊自由權利所必要 20

2.2 Processing is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
資料運用係控管者為遵循其應盡之法定義務，或為公共利益而執行職務，或行使公權力所必要 24

2.2.1 Legal obligation 法定義務 24

2.2.2 Performance of a task carried out in public interest or in the exercise of official authority 為公共利益而執行職務或行使公權力 27
2.3 Reasons of public interest in the area of public health 公共衛生領域之公共利益理由 28
2.4 Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the Right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing 依據第 89(1)條規定，基於公共利益建檔之目的、科學或歷史研究之目的或統計之目的，以第 1 項所規定之權利可能使該運用目的不可能達成或遭嚴重妨礙者為限 30
2.5 Establishment, exercise or defence of legal claims 為建立、行使或防禦法律上之請求 30

The European Data Protection Board
歐盟個人資料保護委員會

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, (hereinafter "GDPR"),
依據歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過保護自然人關於個人資料運用*和自由流通的 2016/679/EU 規則第 70(1)(e)條規定，並廢除第 95/46/EC 號指令（下稱「GDPR」）；

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],
依據歐洲經濟區聯合委員會 2018 年 7 月 6 日第 154/2018 號決定修正的歐洲經濟區合約，特別是其附件 11 及第 37 號議定書[1]；

Having regard to Article 12 and Article 22 of its Rules of Procedure,
依據其議事規則第 12 條和第 22 條，

HAS ADOPTED THE FOLLOWING GUIDELINES

通過以下指引

INTRODUCTION
導言

1. Following the Costeja judgment of the Court of Justice of the European Union ("CJEU") of the 13th of May 2014[2], a data subject may request the provider of an online search engine ("search engine provider")[3], to erase one or more links to web pages from the list of results displayed following a search made on the basis of his or her name.
依據歐盟法院 2014 年 5 月 13 日 Costeja 案件之判決[2]，當事人得請求網路

---

* 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」。

[1] References to "Member States" made throughout these guidelines should be understood as references to "EEA Member States".
本文件所稱「會員國」係指「歐洲經濟區會員國」。

[2] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.
CJEU，C-131/12 案「Google Spain SL 和 Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González」，2014 年 5 月 13 日判決。

[3] including web archives such as archive.org
包括網路檔案館，例如 archive.org。

搜尋引擎供應商（下稱「搜尋引擎供應商」）[3]，刪除以其姓名搜尋而顯示於搜尋結果列表的一個或多個網頁連結。

2. According to Google's Transparency Report[4], the percentage of URLs that Google has not delisted has not increased over the past 5 years since that judgement. However, further to the CJEU judgement, data subjects seem to be more aware of their right to lodge a complaint for refusals of their delisting requests since Supervisory Authorities have observed an increase in the number of complaints regarding the refusal by search engine providers to delist links.
依據 Google 透明度報告[4]，自上述判決作成後五年以來，Google 去列表之網址比率並未增加。但是在歐盟法院上述判決作成後，當事人似乎更意識到如果他們請求刪除遭到拒絕後，其具有提出申訴之權利，監管機關就觀察到申訴搜尋引擎供應商拒絕刪除連結之數量增加。

3. The European Data Protection Board (the "**EDPB**"), in accordance with its Action Plan, is developing guidelines in respect of Article 17 of the General Data Protection Regulation ("**GDPR**"). Until those guidelines are finalised, Supervisory Authorities must continue to handle and investigate, to the extent possible, complaints from data subjects and in a timely manner as possible.
歐盟個人資料保護委員會（下稱「EDPB」）根據其行動計畫，正在擬定與 GDPR 第 17 條有關之指引。在指引定稿之前，監管機關必須繼續盡可能及時處理及調查當事人之申訴。

4. Accordingly, this document aims to interpret the Right to be Forgotten in the search engines cases in light of the provisions of Article 17 GDPR (the "**Right to request delisting**"). Indeed, the Right to be Forgotten has been especially enacted under Article 17 GDPR to take into account the Right to request delisting established in the Costeja judgement.
因此，本文件旨在依據 GDPR 第 17 條規定來解釋搜尋引擎案件中之被遺忘權（下稱「去列表權」）。事實上，被遺忘權是為了回應 Costeja 判決確立之去列表權而制定於 GDPR 第 17 條。

5. Nonetheless, as under the Directive 95/46/EC of 24 October 1995 (the "**Directive**") and as stated by the CJEU in its aforementioned Costeja judgement[5], the Right to request delisting implies two rights (Right to Object

---

[4] https://transparencyreport.google.com/eu-privacy/overview?hl=en

[5] CJEU, Case C-131/12, judgment of 13 May 2014, paragraph 88: *"Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful*".
歐盟法院 2014 年 5 月 13 日 C-131/12 號判決第 88 段：「*第 95/46 號指令第 12(b)條及第 14 條第 1 項(a)款應解*

and Right to Erasure GDPR). Indeed, the application of Article 21 is expressly foreseen as the third ground for the Right to erasure. As a result, both Article 17 and Article 21 GDPR can serve as a legal basis for delisting requests. The right to object and the right to obtain erasure were already granted under the Directive. Nonetheless, as it will be addressed, the wording of the GDPR requires an adjustment of the interpretation of these rights.
儘管如此，根據 1995 年 10 月 24 日第 95/46/EC 號指令（下稱「指令」）以及前述歐盟法院 Costeja 案件之判決[5]，去列表權意指二項權利（GDPR 拒絕權及刪除權）。事實上，第 21 條之適用明顯意在作為行使刪除權之第三個法定事由。因此，GDPR 第 17 條及第 21 條都可作為行使去列表權之法律依據。指令已經賦予拒絕權及刪除權。儘管如此，正如其後之說明，為了符合 GDPR 文義，這些權利之解釋需要調整。

6. As a preliminary point, it should be noted that, while Article 17 GDPR is applicable to all data controllers, this paper focuses solely on processing by search engine providers and delisting requests submitted by data subjects.
首先須指出，雖然 GDPR 第 17 條適用於所有資料控管者，但本指引僅聚焦於搜尋引擎供應商之運用行為及當事人行使之去列表權。

7. There are some considerations when applying Article 17 GDPR in respect of a search engine provider's data processing. In this regard, it is necessary to state that the processing of personal data carried out in the context of the activity of the search engine provider must be distinguished from processing that is carried out by the publishers of the third-party websites such as media outlets that provide online newspaper content[6].
將 GDPR 第 17 條規定適用於搜尋引擎供應商之資料運用時，有一些須考量因素。就此，必須說明在搜尋引擎供應商活動範圍內進行之個人資料運用，必須與第三方網站刊登者（例如，提供網路電子報內容之媒體）進行之運用活動加以區分[6]。

8. If a data subject obtains the delisting of a particular content, this will result in the deletion of that specific content from the list of search results concerning the data subject when the search is, as a main rule, based on his or her name. This content will however still be available using other search criteria.

釋為，為遵守這些法條規定之權利，只要符合這些法條之構成要件，搜尋引擎供應商有義務從依據個人姓名顯示搜尋結果之列表中，刪除由第三方刊登並包含與該個人相關資料之網頁連結，如果該姓名或資料未事先或同時自該等網頁刪除時亦同，甚至在某些情況下，該等網頁刊登之資料本身是合法之情形，亦同。」

[6] CJEU, Case C 131/12, judgment of 13 May 2014; European Court of Human Rights (ECHR), "M.L. and W.W. vs Germany", 28 June 2018.
歐盟法院 2014 年 5 月 13 日 C 131/12 號判決；以及歐洲人權法院（ECHR）2018 年 6 月 28 日「M.L.和 W.W. vs Germany」案件的判決。

當事人請求自列表中刪除特定內容，將使該特定內容從以當事人姓名為搜尋之主要規則之結果列表中刪除。但使用其他搜尋條件仍然可以搜尋到該內容。

9. Delisting requests do not result in the personal data being completely erased. Indeed, the personal data will neither be erased from the source website nor from the index and cache of the search engine provider. For example, a data subject may seek the delisting of personal data from a search engine's index which have originated from a media outlet, such as a newspaper article. In this instance, the link to the personal data may be delisted from the search engine's index; however, the article in question will still remain within the control of the media outlet and may remain publicly available and accessible, even if no longer visible in search results based on queries that include in principle the data subject's name.
行使去列表權不會使個人資料完全被刪除。事實上，個人資料既不會從來源網站刪除，也不會從搜尋引擎供應商之索引及暫存空間（Cache）刪除。例如，當事人可能會尋求從搜尋引擎索引中刪除源自某一媒體之個人資料，例如報紙上之文章。在這個例子中，個人資料之連結可能會從搜尋引擎之索引中刪除；但即使這篇文章在原則上使用當事人姓名查詢之搜尋結果中已不復見，相關文章仍將受該來源媒體控管，並且仍可能處於公眾可使用或存取之狀態。

10. Nevertheless, search engine providers are not exempt in a general manner from the duty to fully erase. In some exceptional cases, they will need to carry out actual and full erasure in their indexes or caches. For example, in the event that search engine providers would stop respecting robots.txt requests implemented by the original publisher, they would actually have a duty to fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name.
然而，搜尋引擎供應商一般而言，不能免除完全刪除之義務。在某些例外情況下，他們必須於索引或暫存空間中執行確實且完整之刪除。例如，如果搜尋引擎供應商不再遵守原始刊登者實施之 robots.txt 要求，他們實際上有責任完全刪除連結至相關內容之 URL，而不只是刪除主要依據當事人姓名搜尋之列表結果。

11. This paper is divided into two topics. The first topic concerns the grounds a data subject can rely on for a delisting request sent to a search engine provider pursuant to Article 17.1 GDPR. The second topic concerns the exceptions to the Right to request delisting according to Article 17.3 GDPR. This paper will be supplemented by an appendix dedicated to the assessment of criteria for handling complaints for refusals of delisting.
本指引分為二個主題。第一個主題是關於當事人得依據 GDPR 第 17.1 條規定向搜尋引擎供應商行使去列表權之事由。第二個主題是關於 GDPR 第

17.3 條規定例外不得行使去列表權之情形。本指引另有一個補充附錄，用以說明評估行使去列表權遭到拒絕之申訴處理標準。

12. This paper does not address Article 17.2[7] GDPR. Indeed, this Article requires data controllers who have made the personal data public to inform controllers who have then reused those personal data through links, copies or replications. Such obligation of information does not apply to search engine providers when they find information containing personal data published or placed on the internet by third parties, index it automatically, store it temporarily and make it available to internet users according to a particular order of preference[8]. In addition, it does not require search engine providers, who have received a data subject's delisting request, to inform the third party which made public that information on the internet. Such obligation seeks to give greater responsibility to original controllers and try to prevent from multiplying data subjects' initiatives. In this regard, the statement by the Article 29 Working Party, saying that search engine providers *"should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some webpages cannot be acceded from the search engine in response to specific queries"* because *"such communication has no legal basis under EU data protection law"*[9] remains valid. It is also planned to have separate specific guidelines in respect of Article 17.2 GDPR.

本指引並不處理 GDPR 第 17.2 條規定[7]。事實上，本條規定要求公開個人資料之資料控管者通知其他透過連結、複製或仿製重新利用這些個人資料之控管者。本條通知義務不適用於搜尋引擎供應商發現第三方在網路上刊登或放置包含個人資料之資訊、自動加入索引、暫時儲存並按照特定之優先順序提供給網路使用者之情形[8]。此外，本條規定亦不要求搜尋引擎供應商在收到當事人行使去列表權時通知在網路上刊登該資料之第三方。本條規定之義務旨在賦予原始控管者更大責任，試圖避免徒增當事人採取之

---

7 Regulation 2016/679 (GDPR), Article 17.2: "*Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those data."*
2016/679 規則(GDPR)第 17.2 條規定：「*如果控管者已公開個人資料，且有義務依據第 1 項規定刪除該個人資料，該控管者應考量現有科技及執行成本採取合理步驟，包括技術上之措施，通知正在處理該個人資料之控管者，當事人已請求這些控管者刪除任何該個人資料之連結或複製或仿製。*」

8 See CJEU, Case C-136/17, GC and Others v CNIL, judgment of 24 September 2019, paragraph 35 and Case C-131/12, judgment of 13 May 2014, paragraph 41.
參見歐盟法院 2019 年 9 月 24 日「GC 和其他人 v CNIL」C-136/17 號判決第 35 段，以及 2014 年 5 月 13 日 C-131/12 號判決第 41 段。

9 Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C131/12, WP 225, 26 November 2014, p. 23.
第 29 條個人資料保護工作小組關於執行歐盟法院「Google Spain and inc v. Agencia Española de Protección de Datos (AEPD)及 Mario Costeja González」C131/12 號判決指引，2014 年 11 月 26 日第 WP 225 號指引，第 23 頁。

行動。對此，第 29 條工作小組之以下說明仍然有效：搜尋引擎供應商「*在通常作法下，不應將網頁因回應特定要求而無法自搜尋引擎造訪之事實，通知那些受去列表行為影響之網站管理員*」，因為「*該通知在歐盟資料保護法之規定下沒有依據*」[9]。目前亦有計劃針對 GDPR 第 17.2 條規定制定不同之具體指引。

1. THE GROUNDS OF THE RIGHT TO REQUEST DELISTING UNDER GDPR
根據 GDPR 行使去列表權之事由

13. The Right to request delisting as provided by Article 17 GDPR does not change the findings of the Costeja judgement, in which the CJEU held that a request for delisting was based on the Right to rectification/erasure and on the Right to object, pursuant to Article 12 and Article 14 of the Directive respectively.
GDPR 第 17 條規定之去列表權沒有改變 Costeja 案之判決見解，在該判決中，歐盟法院認為行使去列表權是依據指令第 12 條及第 14 條規定之更正／刪除權及拒絕權。

14. Article 17.1 sets out a general principle to erase the data in the six following cases:
第 17.1 條規定以下六種應刪除資料情形之一般原則：

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed *(Article 17.1.a);*
個人資料對於蒐集或以其他方式運用之目的而言已無必要（*第 17.1.a 條*）；

b. the data subject withdraws consent on which the processing is based *(Article 17.1.b)*;
當事人撤回運用其個人資料所依據之同意（*第 17.1.b 條*）；

c. the data subject exercised his or her Right to object to processing of his or her personal data pursuant to Article 21.1 and 21.2 GDPR;
當事人依據 GDPR 第 21.1 條及 21.2 條行使拒絕運用其個人資料之權利；

d. the personal data have been unlawfully processed *(Article 17.1.d)*;
個人資料遭違法運用（*第 17.1.d 條*）；

e. the erasure is compliant with a legal obligation *(Article 17.1.e)*;
為了履行法定義務而刪除（*第 17.1.e 條*）；

f. the personal data have been collected in relation to the offer of information society services to a minor *(Article 17.1.f which refers to Article 8.1)*.

個人資料之蒐集與提供未成年人資訊社會服務有關（*指涉第 8.1 條之第 17.1.f 條*）。

15. While all the grounds of Article 17 are theoretically applicable when it comes to delisting, in practice, some will be rarely or never used, such as in case of withdrawal of consent (see ground 2 below).
雖然第 17 條規定之所有事由理論上皆能適用於去列表行為，但實際上，有些很少或從未使用，例如撤回同意之情形（見下文事由 2）。

16. A data subject could however make a delisting request to a search engine provider based on more than one ground. For example, a data subject could request delisting because he or she considers it no longer necessary that his or her personal data are processed by the search engine (Article 17.1.a) and also exercise his or her Right to object to the processing pursuant to Article 21.1 GDPR (Article 17.1.c).
當事人得基於多個事由向搜尋引擎供應商行使去列表權。例如，當事人得主張搜尋引擎已經沒有必要繼續運用其個人資料（第 17.1.a 條），並同時依據 GDPR 第 21.1 條規定行使拒絕權（第 17.1.c 條），從而請求自搜尋結果列表刪除其個人資料。

17. In order for Supervisory Authorities to assess complaints regarding a search engine provider who has refused to erase a particular search result pursuant to Article 17 GDPR, Supervisory Authorities should establish whether the content to which an URL is referring to should be delisted or not. They should thus, in their analysis of the substance of the complaint, take into account the nature of the content made available by the publishers of the third-party websites.
為了使監管機關評估針對搜尋引擎供應商拒絕依據 GDPR 第 17 條規定刪除特定搜尋結果而提出之申訴，監管機關應確認是否應自列表刪除 URL 指涉之內容。因此，他們在分析申訴內容時，應考量第三方網站刊登者提供內容之性質。

1.1 Ground 1: The Right to request delisting when the personal data are no longer necessary in relation to the search engine provider's processing (Article 17.1.a)
事由 1：個人資料對於搜尋引擎之運用活動已經沒有必要而行使去列表權（第 17.1.a 條）

18. According to Article 17.1.a GDPR, a data subject may request a search engine provider, following a search carried out as a general rule on the basis of his or her name, to delist content from its search results, where the data subject's personal data returned in those search results are no longer necessary in relation to the purposes of the processing by the search engine.

依據 GDPR 第 17.1.a 條規定，如果搜尋結果顯示之個人資料，對於搜尋引擎運用目的而言已無必要，當事人得請求搜尋引擎供應商刪除以其姓名作為搜尋之一般規則所取得之搜尋結果內容。

19. This provision enables a data subject to request the delisting of personal information concerning him or her that have been made accessible for longer than it is necessary for the search engine provider's processing. Yet, this processing is notably carried out for the purposes of making information more easily accessible for internet users. Within the context of the Right to request delisting, the balance between the protection of privacy and the interests of Internet users in accessing the information must be undertaken. In particular, it must be assessed whether or not, over the course of time, the personal data have become out-of-date or have not been updated.
本條規定允許當事人於資料開放存取之時間超過搜尋引擎供應商運用資料所必要之時間時，請求去列表化與其相關之個人資料，雖然此種運用主要是為了讓網路使用者更容易存取資料。在當事人行使去列表權之情形下，必須在保護隱私及網路使用者存取資訊之利益間取得平衡。尤其必須評估隨著時間經過，個人資料是否已經過時或未更新。

20. For example, a data subject may exercise his or her Right to request delisting pursuant to Article 17.1.a when:
例如，有下列情形時，當事人得依據第 17.1.a 條規定行使去列表權：

- information about him or her held by a company has been removed from the public register;
公司持有與當事人相關之資料，已從公開登記資料移除；

- a link to a firm's website contains his or her contact details although he or she is no longer working in that firm;
當事人已不在該公司工作，但該公司網站之連結仍包含其詳細之聯絡方式；

- information has to be published on the Internet for a number of years to meet a legal obligation and remained online longer than the time limit specified by the legislation.
資料依法須在網路上刊登數年，但於法律規定之期限經過後仍刊登於網路上。

21. As demonstrated by the examples, a data subject may notably request the delisting of a content where the personal information are obviously inaccurate due to the course of time, or outdated. Such an assessment will incidentally be dependent on the purposes of the original processing. Consequently, the original retention periods of personal data, when available, should also be considered by

Supervisory Authorities when they conduct their analysis of delisting requests pursuant to Article 17.1.a GDPR.
如上述案例所示，當事人可能會特別請求將因時間經過而明顯不正確或過時之個人資料內容去列表化。評估時，將附帶取決於資料原始運用之目的。因此，監管機關依據 GDPR 第 17.1.a 條規定評估去列表之請求時，也應考慮個人資料是否有原始保存期限。

1.2 Ground 2: The Right to request delisting when the data subject withdraws consent where the legal basis for the processing is pursuant to Article 6.1.a or Article 9.2.a GDPR and where there is no other legal basis for the processing (Article 17.1.b)
事由 2：運用行為係依據 GDPR 第 6.1.a 或 9.2.a 條規定之當事人同意，且無其他法定事由，當事人因撤回同意而行使去列表權（第 17.1.b 條）

22. According to Article 17.1.b GDPR, a data subject may obtain the erasure of personal data concerning him or her where he or she withdraws consent for the processing.
根據 GDPR 第 17.1.b 條規定，當事人撤回對其個人資料運用之同意，得請求刪除與其相關之個人資料。

23. In case of delisting, it would mean that the search engine provider would have utilised the consent of the data subject as lawful basis for its processing. Article 17.1 GDPR indeed raises the question of the lawful basis for processing relied upon by a search engine provider for the purpose of returning search engine results including personal data.
於去列表之情形，可能表示搜尋引擎供應商係依據當事人之同意作為運用資料之合法基礎。GDPR 第 17.1 條規定確實引發了搜尋引擎供應商提供含有個人資料之搜尋結果之合法基礎問題。

24. For that reason, it appears unlikely that a delisting request would be submitted by a data subject on the basis that he or she wishes to withdraw consent because the controller to whom the data subject gave his or her consent is the web publisher, not the search engine operator that indexes the data. This interpretation has been endorsed by the CJEU in its judgement C-136-17 of 24 September 2019 (the "**Google 2 judgment**").[10] The Court indicates that *"(...) the consent must be 'specific' and must therefore relate specifically to the processing carried out in connection with the activity of the search engine (...). In practice, it is scarcely conceivable (...) that the operator of a search engine will seek the express*

[10] CJEU, Case C-136/17, Commission nationale de l'informatique et des libertés (CNIL) v. Google LLC, judgment of 24 September 2019.
歐盟法院 2019 年 9 月 24 日「Commission nationale de l'informatique et des libertés (CNIL) v. Google LLC」C-136/17 號判決。

consent of data subjects before processing personal data concerning them for the purposes of his referencing activity. In any event, (...) the mere fact that a person makes a request for de-referencing means, in principle, at least at the time of making the request, that he or she no longer consents to the processing carried out by the operator of the search engine."

因此，當事人似乎不可能藉由希望撤回同意之情形而行使去列表權，因為取得當事人同意之控管者為網路刊登者，而不是把資料編入索引之搜尋引擎供應商。歐盟法院 2019 年 9 月 24 日 C-136-17 號判決（「Google 2 判決」）認同此一解釋[10]。法院指出：「*（……）同意必須是『特定的』，因此必須與搜尋引擎活動相關之運用明確相關（……）。實務上，殊難想像（……）搜尋引擎供應商會為了索引目的而在運用與當事人相關之個人資料前徵求他們的明示同意。無論如何，（……）至少在當事人請求取消索引時即表示，原則上，當事人已不再同意搜尋引擎經營者之運用。*」

25. Nonetheless, in the event where a data subject would have withdrawn his or her consent for the use of his or her data on a particular web page, the original publisher of that web page should inform search engine providers who have indexed that data pursuant to Article 17.2 GDPR. The data subject would thus still be entitled to obtain the delisting of personal data concerning him or her but according to Article 17.1.c in such case.

儘管如此，如果當事人撤回特定網頁使用其資料之同意，該網頁之原始刊登者應依據 GDPR 第 17.2 條規定，通知將資料編入索引之搜尋引擎供應商。因此，當事人在此情形下仍有權利依據第 17.1.c 條規定請求去列表化與其有關之個人資料。

1.3 Ground 3: The Right to request delisting when the data subject has exercised his or her Right to object to the processing of his or her personal data (Article 17.1.c)

事由 3：當事人行使拒絕運用其個人資料之權利而行使去列表權（第 17.1.c 條）

26. Pursuant to Article 17.1.c GDPR, a data subject can obtain from the search engine provider the erasure of personal data concerning him or her where he or she objects to the processing according to Article 21.1 GDPR and where there are no overriding legitimate grounds for the processing by the data controller.

依據 GDPR 第 17.1.c 條規定，如果當事人依據 GDPR 第 21.1 條規定拒絕有關其資料之運用，且資料控管者之運用並無足以凌駕當事人主張之正當事由，則當事人得請求搜尋引擎供應商刪除其個人資料。

27. The Right to object affords stronger safeguards to data subjects since it does not restrict the grounds according to which data subjects may request delisting as under Article 17.1 GDPR.

因為當事人依據 GDPR 第 17.1 條規定行使去列表權之事由並無限制，因此拒絕權為當事人提供了更強而有力之保障。

28. The Right to object to the processing was provided for by Article 14 of the Directive[11] and constituted a ground to request the delisting since the Costeja judgement. However, the differences in the wording of Article 21 GDPR and Article 14 of the Directive suggest that there may also be differences in their application.
以往，拒絕資料運用之權利規定於指令第 14 條[11]，並自 Costeja 判決以來構成行使去列表權之法律依據。但是，GDPR 第 21 條及指令第 14 條的用語不同，表示二者在適用上也可能不同。

29. Under the Directive, the data subject had to base his or her request "*on compelling legitimate grounds relating to his [or her] particular situation"*. In respect of the GDPR, a data subject can object to a processing "*on grounds relating to his or her particular situation*". He or she thus no longer has to demonstrate *"compelling legitimate grounds"*.
當事人以往依據指令之規定提出請求，必須基於「*與其特定處境相關之必要正當事由*」。依據 GDPR 規定，當事人得「*基於與其特定處境有關之事由*」拒絕資料運用。因此，當事人不再需要證明「*必要之正當事由*」。

30. The GDPR therefore changes the burden of proof, providing a presumption in favour of the data subject by obliging on the contrary the controller to demonstrate *"compelling legitimate grounds for the processing"* (Article 21.1). As a result, when a search engine provider receives a request to delist based on the data subject's particular situation, it must now erase the personal data, pursuant to Article 17.1.c GDPR, unless it can demonstrate "*overriding legitimate grounds"* for the listing of the specific search result, which read in conjunction with Article 21.1 are *"compelling legitimate grounds (...) which override the interests, rights and freedoms of the data subject*". The search engine provider can establish any *"overriding legitimate grounds"*, including any exemption provided for under Article 17.3 GDPR. Nonetheless, if the search engine provider fails to demonstrate the existence of overriding legitimate grounds, the data subject is entitled to obtain the delisting pursuant to Article 17.1.c GDPR. As a matter of fact, delisting requests now imply to make the balance between the reasons related to the particular situation of the data subject

[11] Directive 95/46/CE, Article 14: "*Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data*"
95/46/CE 指令第 14 條規定：「*成員國應授予當事人以下權利：(a)除成員國法律另有規定外，至少在第 7(e)及(f)條規定之情形下，在任何時候基於與其特定處境有關之必要正當事由拒絕與其相關之資料運用。如果拒絕有正當事由，控管者之運用行為即不得再涉及該等資料。*」

and the compelling legitimate grounds of the search engine provider. The balance between the protection of privacy and the interests of Internet users in accessing to the information as ruled by the CJEU in the Costeja judgement can be relevant to conduct such assessment, as well as the balance operated by the European Court of Human Rights (ECHR) in press matters.
因此，GDPR 將舉證責任倒置，提供有利於當事人之推定，反過來要求控管者必須證明「運用之必要正當事由」(第 21.1 條)。因此，當搜尋引擎供應商收到當事人基於特定處境行使去列表權時，除非能證明該特定搜尋結果之列表具有「*足以凌駕之正當事由*」，否則即必須依據 GDPR 第 17.1.c 條規定刪除個人資料，此與第 21.1 條規定「*足以凌駕當事人利益、權利及自由之必要正當事由*(……)」應做相同解釋。搜尋引擎供應商可以提出任何「*足以凌駕之正當事由*」，包括 GDPR 第 17.3 條規定之豁免情形。但如果搜尋引擎供應商無法證明具有足以凌駕之正當事由，則當事人即得依據 GDPR 第 17.1.c 條規定取得去列表權。事實上，去列表權現在意指在當事人特定處境與搜尋引擎供應商必要之正當事由間取得平衡。歐盟法院在 Costeja 判決中對於隱私保護與網路使用者存取資訊之利益間所做之權衡，以及歐洲人權法院(ECHR)在媒體事件中所做之利益權衡，可作為上述評估之參考。

31. Therefore, the criteria of delisting developed by the Article 29 Working Party in guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 can still be used by search engine providers and Supervisory Authorities to assess a delisting request based on the Right to object (Article 17.1.c GDPR).
因此，第 29 條工作小組於訂定指引以履行歐盟法院關於「Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González」C-131/12 案件判決，而發展出之行使去列表權標準，仍然可以使用於搜尋引擎供應商及監管機關評估基於拒絕權而行使之去列表權（GDPR 第 17.1.c 條）。

32. In this regard, the "*particular situation*" of the data subject will underlie the delisting request (for example, a search result creates detriment for a data subject when applying for jobs, or undermines his or her reputation in personal life) and will be taken into account when undertaking the balance between personal rights and right to information, in addition to the classic criteria for handling delisting requests, such as:
在這一點上，當事人之「*特定處境*」將構成行使去列表權之基礎（例如，搜尋結果對當事人在應徵工作時造成不利，或傷害個人生活中之名譽），並且除了考慮處理去列表權之典型標準外，也應考慮權衡個人權利及資訊權，例如：

- he or she does not play a role in public life;
  當事人不是公眾人物；
- the information at stake is not related to his or her professional life but affects his or her privacy;
  所涉及之資料與當事人之職業生活無關，但會影響其隱私；
- the information constitutes hate speech, slander, libel or similar offences in the area of expression against him or her pursuant to a court order;
  依據法院命令，資料之表達構成針對當事人之仇恨言論、詆毀、誹謗或類似罪行；
- the data appears to be a verified fact but is factually inaccurate;
  資料看起來是經過驗證之事實，但其實不正確；
- the data relates to a relatively minor criminal offence that happened a long time ago and causes prejudice to the data subject.
  資料與很久以前相當輕微之刑事犯罪有關，導致對當事人之偏見。

33. Nonetheless, these criteria won't have to be examined in the absence of proof of compelling legitimate grounds to refuse the request.
儘管如此，如果控管者不能證明有必要之正當事由可拒絕當事人行使去列表權，上述標準即無須列入審查。

1.4 Ground 4: The Right to request delisting when the personal data have been unlawfully processed (Article 17.1.d)
事由 4：個人資料遭違法運用而行使去列表權（第 17.1.d 條）

34. According to Article 17.1.d GDPR, a data subject may request the erasure of personal data concerning him or her in the instance where they have been unlawfully processed.
根據 GDPR 第 17.1.d 條規定，如果個人資料遭違法運用，當事人得請求刪除與其相關之個人資料。

35. The notion of unlawful processing shall first be interpreted in view of Article 6 GDPR dedicated to lawfulness of processing. Other principles established under the GDPR (such as principles of Article 5 GDPR or of other provisions of Chapter II) may serve such interpretation.
首先，違法運用之概念應依據專門針對運用資料合法性之 GDPR 第 6 條加以解釋。其他依據 GDPR 確立之原則（例如 GDPR 第 5 條或第二章其他規定揭櫫之原則）皆可用來解釋這個概念。

36. This notion shall secondly be interpreted broadly, as the infringement of a legal provision other than the GDPR. Such interpretation must be conducted

objectively by Supervisory Authorities, according to national laws or to a court decision. For instance, a delisting request shall be granted in the event where the listing of personal information has been expressly prohibited by a court order.
其次，此一概念應作廣義解釋，包括違反 GDPR 以外之法律規定。這種解釋必須由監管機關依據國家法律或法院判決客觀進行。例如，如果法院命令明確禁止個人資料列表，即應同意去列表之請求。

In cases where a search engine provider is not able to demonstrate a legal basis for its processing, a delisting request may fall under the scope of art 17.1.d GDPR, as the processing of personal data in such cases must be considered unlawful. Nonetheless, it must be reminded that in case of unlawfulness of the original processing, the data subject remains entitled to request delisting under Article 17.1.c GDPR.
如果搜尋引擎供應商無法證明其運用資料之法律依據，去列表請求可能落入 GDPR 第 17.1.d 條規定之適用範圍，在此情況下，個人資料之運用必須被視為違法。但應注意當事人對於自始即屬違法之資料運用，仍然可以依據 GDPR 第 17.1.c 條規定行使去列表權。

1.5 Ground 5: The Right to request delisting when the personal data have to be erased for compliance with a legal obligation (Article 17.1.e)
事由 5：為遵守法定義務而有必要刪除個人資料之去列表權（第 17.1.e 條）

37. According to Article 17.1.e GDPR, a data subject may request a search engine provider to delist one or more search results if the personal data need to be erased in compliance with a legal obligation in Union or Member State Law to which the search engine provider is subject.
依據 GDPR 第 17.1.e 條規定，如果搜尋引擎供應商依據歐盟或成員國法律負有法定義務必須刪除個人資料，則當事人可以請求搜尋引擎供應商刪除一個或多個搜尋結果。

38. Compliance with a legal obligation may result from an injunction, an express request by national or EU law for being under a “legal obligation to erase” or the mere breach by the search engine provider of the retention period. For illustrative purposes, the retention period of data is set by a text but would not be complied with (but this hypothesis mainly concerns public files). This case could maybe encompass the hypothesis of non-anonymized or identifying data available in open data.
遵守法定義務可能源於法院禁制令、國家或歐盟法律明文規定「刪除之法定義務」，或只是搜尋引擎供應商違反保存期限。舉例而言，資料之保存期限業經明文規定，但沒有被遵守（但這個假設主要涉及公共檔案）。這個情況可能包括假設可於開放資料存取之非匿名資料或足以識別當事人之資料的情形。

1.6 Ground 6: The Right to request delisting when the personal data have been collected in relation to the offer of information society services (ISS) to a child (Article 17.1.f)
事由 6：個人資料之蒐集與提供「資訊社會服務」（ISS）給兒童有關而行使去列表權（第 17.1.f 條）

39. According to Article 17.1.f GDPR, a data subject may request a search engine provider to delist one or more results if personal data have been collected in relation to the offer of ISS to a child referred to in Article 8.1 GDPR.
根據 GDPR 第 17.1.f 條規定，如果是 GDPR 第 8.1 條規定與提供 ISS 給兒童有關而蒐集之個人資料，當事人可以請求搜尋引擎供應商刪除一個或多個搜尋結果。

40. The Article covers the direct provision of ISS and no other types of processing. The GDPR does not define ISS; rather, it refers to existing definitions in EU law[12]. There are some difficulties in interpretation as Recital 18 of Directive 2000/31/CE of the European Parliament and of the Council of June 8, 2000 provides a definition both broad and ambiguous of the notion of *"the direct provision of information society services"*. It mainly indicates that these services *"span a wide range of economic activities which take place on-line*", but specifies that they are not restricted to *"services giving rise to on-line contracting but also, in* ***so far as they represent an economic activity****, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data",* outlining the criteria of economic activity.
本條涵蓋 ISS 之直接提供行為，不包括其他類型之資料運用。GDPR 沒有定義 ISS，而是援引歐盟法律中之既有定義[12]。由於歐洲議會及理事會 2000 年 6 月 8 日通過之 2000/31/CE 指令前言第 18 段對「*直接提供資訊社會服務*」概念之定義廣泛且模糊，因此在解釋上有些困難。前言主要表明這些服務「*涵蓋了發生於網路上之諸多經濟活動*」，但指出這些活動不限於「*帶來線上訂約之服務，****只要是經濟活動****，也涵蓋接受方沒有付費之服務，例如，提供線上資訊或商業通訊之服務，或提供可以搜尋、存取及檢索資料工具之服務*」，此概述了經濟活動之標準。

41. It stems from the above that search engine providers' activities are likely to fall within the scope of direct provision of ISS. Nonetheless, search engine providers

[12] Specifically, Article 1(1)(b) of 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 (codification).
具體而言，歐洲議會和理事會 2015 年 9 月 9 日通過建立在技術法規領域提供資訊之程序和資訊社會服務（編纂）規則之指令 2015/1535 第 1(1)(b)條規定。

do not question whether the personal data they are indexing concern or not a child. Yet, in view of their specific responsibilities, and subject to the application of Article 17.3 GDPR, they would have to delist a content relating to a child pursuant to Article 17.1.c GDPR, acknowledging that being a child is a valid "ground relating to a particular situation" (Article 21 GDPR) and that *"children merit specific protection with regard to their personal data"* (Recital 38 GDPR). In such case, the context of the collection of personal data by the original controller must be considered. In particular, the date of the beginning of the processing by the original website must be taken into account when a data subject requests the delisting of a content.
綜上所述，搜尋引擎供應商之活動可能落入直接提供 ISS 之範圍。儘管如此，搜尋引擎供應商不會質疑他們編入索引之個人資料是否涉及兒童。然而，考量搜尋引擎供應商之特定責任且必須遵守 GDPR 第 17.3 條之規定，他們必須依據 GDPR 第 17.1.c 條規定自搜尋列表刪除與兒童有關之內容，肯認作為兒童是一個有效之「與特定處境相關之事由」(GDPR 第 21 條)以及「*兒童應就其個人資料獲得特別保護*」(GDPR 前言第 38 段)。在此情形下，必須考慮原始控管者蒐集個人資料之情境。尤其是，當事人請求刪除內容時，必須考慮原始網站開始運用資料之日期。

2. THE EXCEPTIONS TO THE RIGHT TO REQUEST DELISTING UNDER ARTICLE 17.3
依據第 17.3 條規定行使去列表權之例外

42. Article 17.3 GDPR states that paragraphs 1 and 2 of Article 17 GDPR will not apply when processing is necessary:
GDPR 第 17.3 條規定，第 17 條第 1 項及第 2 項規定不適用於有必要運用資料之下列情形：

a. for exercising the right of freedom of expression and information *(Article 17.3.a);*
為行使表意及資訊自由之權利（第 17.3.a 條）；

b. for compliance with a legal obligation that requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller *(Article 17.3.b);*
控管者為遵守歐盟或成員國法律規定之法定義務而運用資料，或為公共利益執行職務，或為了行使賦予控管者之公權力（*第 17.3.b 條)*；

c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9.2 as well as Article 9.3 *(Article 17.3.c);*

依據第 9.2 條(h)與(i)點及第 9.3 條（第 17.3.c 條）規定，為公共衛生領域之公共利益；

d. for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing *(Article 17.3.d);* or
依據第 89(1)條規定，基於為公共利益建檔之目的、科學或歷史研究之目的或統計之目的，但以第 1 項規定之權利可能使該運用之目的不可能達成或嚴重損害該目的之實現者為限*（第 17.3.d 條）*；或者

e. for the establishment, exercise or defense of legal claims *(Article 17.3.e).*
為建立、行使或防禦法律上之請求*（第 17.3.e 條）*。

43. This part aims to demonstrate that most of the exceptions under Article 17.3 GDPR do not appear suitable in case of a delisting request. Such inadequacy pleads in favor of the application of Article 21 GDPR for delisting requests. In any event, it must be remembered that exceptions provided for under Article 17.3 GDPR can be invoked as compelling legitimate grounds pursuant to Article 17.1.c GDPR.
本部分旨在說明 GDPR 第 17.3 條規定之大多數例外情況，似乎不適合用於去列表之請求。這些不適合的情況，有利於將 GDPR 第 21 條規定適用於去列表之請求。無論如何，必須記住，引用 GDPR 第 17.3 條規定之例外情況，可以作為 GDPR 第 17.1.c 條規定所稱之必要正當事由。

2.1 Processing is necessary for exercising the right of freedom of expression and information
資料運用係行使表意與資訊自由權利所必要

44. This exemption to the application of Article 17.1 GDPR must be interpreted and applied in the context of the characteristics that define erasure. Article 17.1 GDPR is described as a clear and unconditional mandate addressed to controllers. If the conditions set forth in Article 17.1 GDPR are met, the controller shall *"have the obligation to delete personal data without undue delay"*. Nonetheless, this is not an absolute right. The exemptions of Article 17.3 GDPR identify cases in which this obligation does not apply.
此豁免 GDPR 第 17.1 條規定之情況，必須放到討論刪除定義要件之脈絡下解釋及適用。GDPR 第 17.1 條規定，是對控管者明確且無條件之要求。一旦符合 GDPR 第 17.1 條規定之要件，控管者應「*有義務刪除個人資料，不得無故拖延*」。儘管如此，這不是絕對權利。GDPR 第 17.3 條規定說明不適用該義務之豁免情形。

45. However, the balance between protecting the rights of interested parties and freedom of expression, including free access to information, is an intrinsic part of Article 17 GDPR.
然而，在保護利害關係人權利與保護表意自由—包括存取資料之自由—間取得平衡，是 GDPR 第 17 條規定之必要內涵。

46. The CJEU recognised in the Costeja judgement and repeated recently in the Google 2 judgment that the processing carried out by a search engine provider can significantly affect the fundamental rights to privacy and data protection law when the search is performed using the name of a data subject.
歐盟法院在 Costeja 案件之判決認可並在最近之 Google 2 判決重申，搜尋引擎供應商以當事人姓名作為搜尋方法之運用行為，可能嚴重影響隱私之基本權利及個資保護法。

47. When weighing up the rights and freedoms of data subjects and the interests of Internet users in accessing the information through the search engine provider, the Court understood that *"Whilst it is true that the data subject's rights are protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."*[13]
權衡當事人之權利及自由，以及網路使用者透過搜尋引擎供應商存取資料之利益時，法院瞭解「*雖然當事人受這些法條保護之權利，一般來說確實凌駕於網路使用者之利益，但於特定情形，此種平衡可能取決於個案資料之性質、該資料對當事人私生活之敏感程度、以及公眾獲得該資料之利益，這個利益—特別是依據當事人於公共生活中所扮演之角色—可能會有所不同*」[13]。

48. The Court also considered that the rights of the data subjects will prevail, in general[14], on the interest of Internet users in accessing information through the search engine provider. However, it identified several factors that may influence such determination. Among them include: the nature of the information or its sensitivity, and especially the interest of Internet users in accessing information, an interest that can vary depending on the role played by the interested party in public life.

---

[13] CJEU, C-131/12, judgment of 13 May 2014, paragraph 81; CJEU, C-136/17, judgment of 24 September 2019, paragraph 66.
歐盟法院 2014 年 5 月 13 日 C-131/12 案判決第 81 段；歐盟法院 2019 年 9 月 24 日 C-136/17 案判決第 66 段。

[14] CJEU, Case C-131/12, judgment of 13 May 2014, paragraph 99; CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 53.
歐盟法院 2014 年 5 月 13 日 C-131/12 案判決第 99 段；歐盟法院 2019 年 9 月 24 日 C-136/17 案判決第 53 段。

法院也認為，一般而言[14]，當事人之權利優先於網路使用者透過搜尋引擎供應商存取資料之利益。但法院也確認了數個可能影響此種判定之因素。其中包括：資料之性質或其敏感性，尤其是網路使用者存取資料之利益，這種利益可能因利害關係人於公共生活中所扮演之角色而異。

49. The analysis of the delisting by the Court implies that, when assessing requests for delisting, the decision on the maintenance or blocking of the search results by a search engine provider necessarily has to consider what would be the impact of a delisting decision on the access to information by Internet users[15]. This impact does not necessarily entail the rejection of a delisting request. As confirmed by the Court, such interference with the fundamental rights of the data subject has to be justified by the preponderant interest of the general public in having access to the information in question.
法院對於去列表權的分析，意味著在評估去列表請求，搜尋引擎供應商決定維持或封鎖特定搜尋結果時，必須考慮該去列表之決定對網路使用者存取資料之影響[15]。此種影響不必然導致去列表請求遭拒。正如法院所確認，此種對當事人基本權利之干涉，必須以公眾於存取案關資料上具有優勢利益為正當理由。

50. The Court also distinguished between the legitimacy that a web publisher can have to disseminate information against the legitimacy of the search engine provider. The Court recognised that the activity of a web publisher can be undertaken exclusively for the purposes of journalism, in which case the web publisher would benefit from the exemptions that Member States could establish in these cases on the basis of Article 9 of the Directive (currently , Article 85.2 GDPR). In this regard, in the judgment *"M.L. and W.W. vs Germany"* of June 28th, 2018, the ECHR indicates that the balancing of the interests at issue may lead to different results depending on the request at stake (distinguishing (i) a request for erasure brought against the original publisher whose activity is at the heart of what freedom of expression aims to protect from (ii) a request brought against the search engine whose first interest is not to publish the original information on the data subject but notably to enable identifying any available information on this person and thus establishing his or her profile).
法院也區分網路刊登者傳播資訊之正當性及搜尋引擎供應商之正當性。法院認可，網路刊登者之活動可以完全出於新聞工作之目的，在此情形下，網路刊登者將受益於成員國可以針對這些情形依據指令第 9 條（即現行 GDPR 第 85.2 條）規定制定豁免之情形。對此，歐洲人權法院 2018 年 6 月 28 日「M.L.和 W.W vs Germany」案件之判決指出，依據個案請求之不同，特定案件中之利益權衡可能導致不同之結果（區分(i)請求原始刊登者

[15] 歐盟法院, Case C-136/17, judgment of 24 September 2019, paragraph 56 et seq..
歐盟法院，C-136/17 案，2019 年 9 月 24 日判決，第 56 段以下。

刪除，而該刊登者之活動乃表意自由旨在保護之核心；(ii)請求搜尋引擎刪除，而該搜尋引擎之首要利益並非刊登有關當事人之原始資料，而是能夠明顯識別有關此人之任何可用資料，從而建立該人之個人檔案）。

51. Those considerations should be assessed in respect of Article 17 GDPR complaints as in those decisions, the rights of the data subjects that have requested the delisting must be weighed with the interests of Internet users to access the information.

依據 GDPR 第 17 條規定對於申訴作成決定時應評估上述考量，因為這些決定必須權衡行使去列表權之當事人權利與網路使用者存取資料之利益。

52. As explained by the CJEU in its Google 2 judgment, Article 17.3.a GDPR is *"an expression of the fact that the right to protection of personal data is not an absolute right but (...) must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"*.[16] It *"expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other."*[17]

正如歐盟法院於 Google 2 判決之闡釋，GDPR 第 17.3.a 條「*希望傳達一個事實，保護個人資料不是絕對權，而是（……）必須依據比例原則，審酌該權利之社會功能，並與其他基本權利取得平衡*」[16]。本條「*明確規定應在《憲章》第 7 條及第 8 條保障之隱私和個人資料保護之基本權利，以及《憲章》第 11 條保障之資訊自由基本權利間取得平衡。*」[17]

53. The Court concludes that *"where the operator of a search engine has received a request for dereferencing relating to a link to a web page on which personal data falling within the special categories (...), the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter, ascertain, having regard to the reasons of substantial public interest (...), whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject's name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the*

---

[16] CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 57.
歐盟法院 2019 年 9 月 24 日 C-136/17 號判決第 57 段。

[17] CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 59.
歐盟法院 2019 年 9 月 24 日 C-136/17 號判決第 59 段。

Charter."[18]

法院結論是，「*如果搜尋引擎供應商接到取消連結至某一個網頁之請求，而該網頁上之個人資料屬於特種類別（……），供應商必須根據該請求之所有相關因素，審酌對於憲章第 7 條及第 8 條保障之當事人隱私及個人資料保護之基本權利受到干擾之嚴重性，確實考量重大公共利益之理由（……），查明是否有絕對必要將該連結包含在根據當事人姓名進行搜尋所顯示之結果列表中，以保護可能有興趣透過這種搜尋方式存取該網頁之網路使用者受憲章第 11 條保護之資訊自由。*」[18]

54. To conclude, depending on the circumstances of the case, search engine providers may refuse to delist a content in the event where they can demonstrate that its inclusion in the list of results is strictly necessary for protecting the freedom of information of internet users.

結論是，根據個案情形，如果搜尋引擎供應商能證明將某內容列入結果列表對於保護網路使用者之資訊自由有絕對必要，即得拒絕將該內容去列表。

2.2 Processing is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller 資料運用係控管者為遵循其應盡之法定義務，或為公共利益而執行職務，或行使公權力所必要

55. The content of this exemption makes it difficult to apply to the activity of search engine providers and it may have influence on the decisions of delisting certain results, as the processing of data by search engine providers is based, in principle, on the legitimate interest of the search engine provider.

原則上，搜尋引擎供應商運用資料係基於其正當利益，因此這個豁免內容難以適用於搜尋引擎供應商之活動，且可能對將某些結果去列表之決定產生影響。

2.2.1 Legal obligation 法定義務

56. It is difficult to imagine the existence of legal provisions that oblige search engine providers to disseminate certain information. This is a consequence of the type of activity they develop. Search engine providers do not produce or present information.

---

[18] CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 69.
歐盟法院 2019 年 9 月 24 日 C-136/17 號判決第 69 段。

殊難想像會有法律課予搜尋引擎供應商散布某些資訊之義務。散布資訊是搜尋引擎供應商發展活動類型之結果。搜尋引擎供應商本身並不製造或呈現這些資訊。

57. Therefore, it seems unlikely that Member State law includes obligations for search engine providers to publish some type of information, instead of setting the obligation for that publication to be carried out in other web pages that will then be linked by search engine providers.
因此，成員國法律似乎不太可能課予搜尋引擎供應商應刊登某種類型資料之義務，比較可能將應刊登義務加諸於其他網頁，再由搜尋引擎供應商連結到這些網頁。

58. This assessment may also be extended to the possibility that Union or Member State law enables a public authority to take decisions that oblige search engine providers to publish information directly, and not through the URL links to the web page where that information is contained.
此種評估還可以延伸至歐盟或成員國法律是否可能允許公務機關作成處分，課予搜尋引擎供應商直接刊登資料之義務，而非課予他們連結到包含該資訊之 URL 網頁之義務。

59. If there are cases in which the law of a Member State establishes the obligation for the search engine providers to publish decisions or documents containing personal information, or which authorises public authorities to demand such publication, the exemption contained in Article 17.3.b GDPR should be applied.
如果成員國法律規定搜尋引擎供應商有義務刊登包含個人資料在內之決定或文件，或者授權公務機關要求刊登，則應適用 GDPR 第 17.3.b 條之豁免規定。

60. This application must take into account the terms in which it is established, that is, that the maintenance of the information in questions is necessary to meet the legal obligation of publication. For example, that a legal obligation, or the decision of an authority legally entitled to adopt it, may include a time limit to the publication, or expressly stated purposes that may have been reached within a certain time period. In these cases, if the request for delisting occurs having exceeded these time limits, it should be considered that the exemption is no longer applicable.
上述適用方式必須考慮其所依據之法條，亦即為了符合刊登之法定義務有必要保存相關資料。例如，法定義務或具有法定權限之機關作成之決定，可能包括刊登之期限，或明確說明於特定期限內可達到之目的。在這些情況下，如果期限屆滿後才提出去列表之請求，應視為不再適用豁免情形。

61. On the contrary, it is frequent that Member State law provides for the publication on web pages of information containing personal data. That legal obligation to

publish or maintain the published information cannot be considered as covered by the exemption contained in Article 17.3.b GDPR, since it is not directed to the search engine provider, but to the web publishers whose content is linked by the search engine provider's index. Therefore, the search engine provider cannot invoke the existence of the obligation to reject a request for delisting.
相反地，成員國法律經常規定網頁上應刊載包含個人資料之資訊。要求刊登或保留已刊登資訊之法定義務，不能被視為包含在 GDPR 第 17.3.b 條規定之豁免情形，因為這不是針對搜尋引擎供應商，而是針對其內容被連結至搜尋引擎供應商索引之網路刊登者。因此，搜尋引擎供應商不得援引這個義務而拒絕當事人行使去列表權。

62. However, the legal obligation of publication addressed to other web publishers should be taken into consideration when establishing the balance between the rights of data subjects and the interest of the Internet users in accessing the information. The fact that information must be published online by legal mandate, or following the decision of an authority legally entitled to adopt it, is indicative of an interest in the public being able to access that information.
但是，在當事人權利及網路使用者存取資料之利益間進行權衡時，應考慮其他網路刊登者法律上之刊登義務。依據法律規定或享有法定權限之主管機關作成之決定必須在網路上刊登資料之事實，顯示公眾享有存取資料之利益。

63. That presumption of existence of a prevalent interest of the public does not operate in the same way in respect of the originating web pages compared to the results index of a search engine provider. Although the legal obligation to publish information on a certain web site may lead to the conclusion that this information should not be deleted from that web page, the decision regarding the results offered by the search engine provider when the name of a data subject is generally used as search term may be different.
就公眾是否享有優勢利益之問題，在原始網頁與搜尋引擎供應商提供搜尋結果索引之間，容有不同之判斷。雖然在網站上刊登資料之法定義務，可能得出不應該從網頁刪除資料之結論，但在當事人姓名被經常性地作為搜尋條件而使用時，針對搜尋引擎供應商所提供之搜尋結果所作出之評斷可能有所不同。

64. The assessment of the request for delisting in these cases should not assume that the existence of the legal obligation of publication necessarily implies that, to the extent that this obligation is imposed on the original web publishers, it is not possible to accept the delisting by the search engine provider.
評估這些情形之去列表請求時，不應假設課予原始網頁刊登者刊登內容之法定義務，必然意味著搜尋引擎供應商不可能接受去列表之請求。

65. The decision should be taken, as is the general rule, by balancing the rights of the data subject and the interest of the Internet users to access this information through the search engine provider.
一般來說，作成決定時，應權衡當事人之權利及網路使用者透過搜尋引擎供應商存取資料之利益。

2.2.2 Performance of a task carried out in public interest or in the exercise of official authority
為公共利益而執行職務或行使公權力

66. Search engine providers are not public authorities and therefore do not exercise public powers by themselves.
搜尋引擎供應商並非公務機關，因此自己不行使公權力。

67. However, they could exercise those powers if they were attributed by the law of a Member State or of the Union. In the same way that they could carry out missions of public interest if their activity was considered necessary to satisfy that public interest in accordance with national legislation[19].
但如果成員國或歐盟法律賦予他們這些權力，搜尋引擎供應商可以行使這些權力。同樣地，如果搜尋引擎供應商之活動被認為是依據國家法律滿足公共利益所必須，他們可以執行公共利益任務[19]。

68. Given the characteristics of search engine providers, it is unlikely that Member States will grant them public powers or consider that their activity or part of it is necessary for the achievement of a legally established public interest.
考量搜尋引擎供應商之特點，成員國不太可能授予搜尋引擎供應商公權力，或認為其活動或部分活動對於實現法律所確立之公共利益是必要的。

69. If, in spite of that, there is a case in which the law of the Member States grants search engines public powers or links their activity to the achievement of a public interest, they could avail of the exemption provided for in Article 17.3.b GDPR. The considerations previously made on the cases in which the law of a Member State had established a legal obligation to process information for search engine providers are also valid in this case.
儘管如此，如果成員國法律授予搜尋引擎公權力或將其活動與實現公共利益相連結，搜尋引擎可以援引 GDPR 第 17.3 b 條規定之豁免事由。先前針

[19] GDPR, Article 6.3: "The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or
(b) Member State law to which the controller is subject (…)"
GDPR 第 6.3 條規定：「第 1 項(c)和(e)點所定之運用基礎應為：
(a) 歐盟法律；或
(b) 控管者適用之成員國法律（……）」

對成員國法律規定搜尋引擎供應商具有運用資料之法定義務之案例中所做之考量，在本案例中同樣成立。

70. To decide not to follow a delisting request for reasons related to this exemption, it is necessary to determine whether the maintenance of the information in the search engine results is necessary for the achievement of the public interest pursued or for the exercise of the powers of attorney.
決定因本項豁免事由而拒絕去列表之請求時，必須確定保存於搜尋引擎搜尋結果中之資料，對於達成所欲追求之公共利益或對行使權力是必要的。

71. On the other hand, the legal definition of powers or public interest would be carried out by a Member State, and if the search engine rejects a request for delisting on the basis of this exemption, it must also be understood that it does so because it considers that its activity is necessary to achieve public interests. The search engine provider should, in that event, provide reasons why it considers its activity to be carried out in the public interest. Without such an explanation, the denial to follow a data subject's delisting request does not have the possibility of relying on the exemption.
另一方面，權力或公共利益由成員國法律來定義，如果搜尋引擎基於此項豁免事由拒絕去列表之請求，也必須理解為，搜尋引擎這樣做是因為搜尋引擎認為其活動係實現公共利益所必要。在這種情形下，搜尋引擎供應商應提出其認為活動係基於公共利益而執行之理由。如果欠缺這樣之解釋，拒絕當事人去列表之請求時，即不得援引此項豁免事由。

72. Consequently, it would also be the Supervisory Authority of the Member State whose law is applicable that will have to deal with a potential complaint pursuant to Article 55.2 GDPR.
因此，根據 GDPR 第 55.2 條，也將由制定相關法律之成員國監管機關受理可能之申訴。

2.3 Reasons of public interest in the area of public health
公共衛生領域之公共利益理由

73. This exemption is a specific case based on the fact that processing is necessary for the performance of a public interest.
此項豁免乃資料之運用係為履行公共利益所必要之具體案例。

74. In this case, the public interest is limited to the area of public health, but, as with the public interest in any other area, the lawful basis for the processing must be established in Union law or Member State law.
於此種情形，公共利益僅限於公共衛生領域，但與任何其他領域之公共利益一樣，必須在歐盟法律或成員國法律中確立運用資料之合法基礎。

75. From the point of view of the application of this exemption in the context of the activity of the search engine provider, the same conclusions as stated above can be reached. It does not seem likely that the law of a Member State or of the Union can establish a relationship between the activity of the search engine provider and the maintenance of information or of a category of information in the results of the search engine provider with the achievement of purposes of public interest in respect of public health.
將此項豁免事由適用於搜尋引擎供應商之活動時，亦可得出與上述相同之結論。成員國法律或歐盟法律似乎不太可能確立搜尋引擎供應商之活動，與為了公共衛生領域之公共利益目的而於搜尋引擎供應商之搜尋結果中保留資料或某類資料間，具有一定關係。

76. This conclusion is more evident if one takes into account that the effect of delisting is only that some results are deleted from the results page that is obtained when mainly a name is entered as a search criterion. But the information is not deleted from the search engine providers' indexes and can be retrieved using other search terms.
如果考量去列表之影響在於僅刪除以輸入姓名作為搜索標準時獲得之結果頁面，此一結論就更明顯了。但這些資料不會自搜尋引擎供應商之索引中刪除，而且可以透過其他搜尋條件檢索取得。

77. It is, therefore, difficult to imagine that keeping those results visible when searches are mainly made on the basis of a data subject's name can be considered, in general, as something necessary for reasons of public interest in the area of public health.
因此，殊難想像在主要以當事人姓名進行搜尋的情況下，保留這些搜尋結果是為了公共衛生領域之公共利益所必要。

78. The criteria on the applicability of national standards and the identification of the Supervisory Authority that must deal with possible claims in a case relating to Article 17 GDPR that was rejected using this exemption have been discussed above.
上文已經討論過國家判準之適用，並確認因適用此項豁免事由而使關於 GDPR 第 17 條之去列表權遭到拒絕後受理可能提起之申訴之監管機關。

2.4 Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the Right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing
依據第 89(1)條規定，基於公共利益建檔之目的、科學或歷史研究之目的或統計之目的，以第 1 項所規定之權利可能使該運用目的不可能達成或遭嚴重妨礙者為限

79. In this scenario, the search engine provider must be able to demonstrate that the delisting of a certain content on the results page is a serious obstacle or completely prevents the achievement of scientific or historical research purposes or statistical purposes.
在此種情形下，搜尋引擎供應商必須證明自結果頁面上刪除某些內容將嚴重妨礙或完全阻礙科學或歷史研究目的或統計目的之實現。

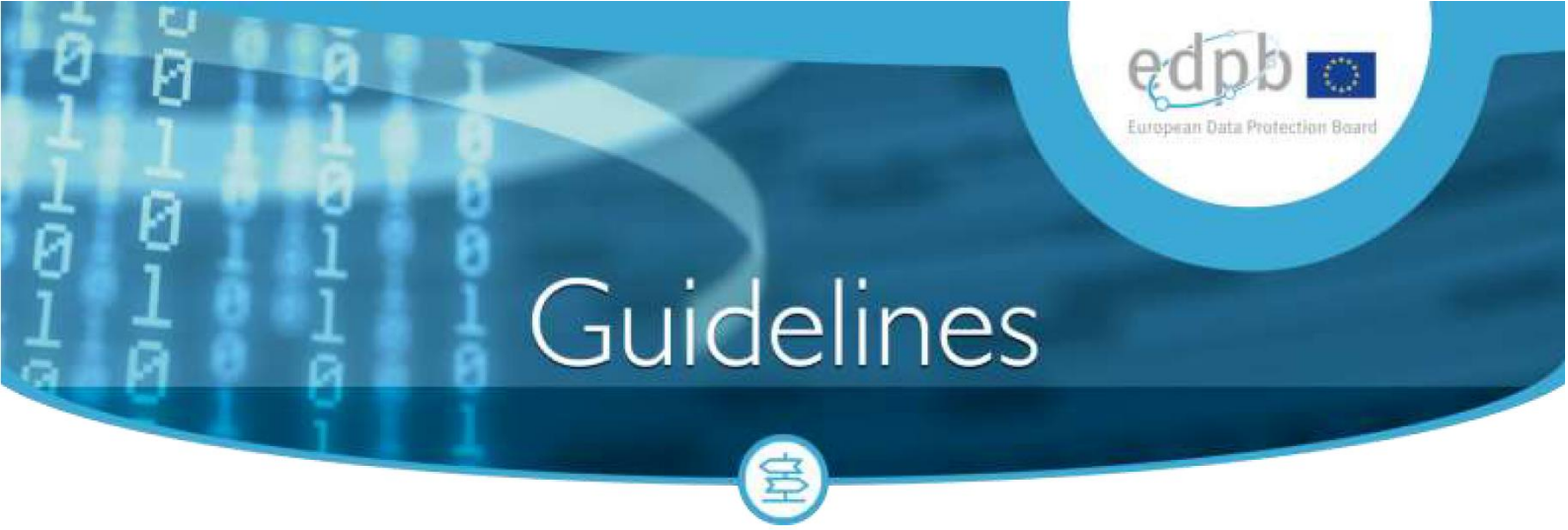
80. It should be understood that these purposes must be objectively pursued by the search engine provider. The possibility that the suppression of results could significantly affect research purposes or statistical purposes pursued by users of the search engine provider's service is not relevant for the application of this exemption. Those purposes, if they exist, should be taken into consideration when establishing a balance between the rights of the data subject and the interests of the Internet users in accessing the information through the search engine provider.
應當瞭解，搜尋引擎供應商必須客觀地追求這些目的。即使限制搜尋結果可能顯著影響搜尋引擎供應商服務用戶所追求之研究或統計目的，亦與此項豁免事由之適用無關。如果該等目的存在，應於衡量當事人之權利與網路使用者透過搜尋引擎供應商存取資料之利益時加以考量。

81. It must also be noted that these purposes may be objectively pursued by the search engine provider, without a link between in principle the name of the data subject and the search results being necessary.
另須注意，搜尋引擎供應商亦得在客觀上達成這些目的，原則上並無必要將當事人姓名與搜索結果相連結。

2.5 Establishment, exercise or defence of legal claims
為建立、行使或防禦法律上之請求

82. In principle, it is very unlikely that search engine providers can use this exemption to reject Article 17 GDPR delisting requests.
原則上，搜尋引擎供應商不太可能利用此一豁免事由拒絕依據 GDPR 第 17 條規定之去列表請求。

83. It must be further emphasised that a delisting request supposes the suppression of certain results from the search results page provided by the search engine provider when the name of a data subject is normally used as search criteria. The information remains accessible using other search terms.
必須進一步強調，去列表之請求係預設在通常以當事人姓名作為搜尋條件時，從搜尋引擎供商提供之搜尋結果頁面中隱去某些結果。如果使用其他搜尋條件時，仍然可以取得這些資料。



Guidelines 01/2022 on data subject rights - Right of access
當事人權利－近用權指引 01/2022

Version 1.0
第 1.0 版

Adopted on 18 January 2022
2022 年 1 月 18 日通過

EXECUTIVE SUMMARY
摘要

The right of access of data subjects is enshrined in Arti. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection legal framework since its beginning and is now further developed by more specified and precise rules in Art. 15 GDPR.
當事人之近用權體現於歐盟基本權利憲章第 8 條，自始屬於歐洲資料保護法律框架之一部分，現由一般資料保護規則（下稱「GDPR」）第 15 條為更具體、精確之進一步規範。

Aim and overall structure of the right of access
近用權之目標及整體架構

The overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. This will make it easier - but is not a condition - for the individual to exercise other rights such as the right to erasure or rectification.
近用權之整體目標係為個人提供充分、透明且易近用之個人資料運用*資訊，使當事人得以知悉及查驗運用之合法性及被運用資料之正確性。當事人亦將因近用權而能夠更容易行使其他權利（但近用權並非行使其他權利的要件），如刪除或更正之權利。

The right of access according to data protection law is to be distinguished from similar rights with other objectives, for example the right of access to public documents which aims at guaranteeing transparency in public authorities' decision-making and good administrative practice.
資料保護法律下之近用權應與具有其他目標的類似權利有所區隔；舉例而言，公共文書近用權旨在確保公務機關決策之公開透明及良好的行政實踐。

However, the data subject does not have to give reasons for the access request and it is not up to the controller to analyse whether the request will actually help the data subject to verify the lawfulness of the relevant processing or exercise other rights. The controller will have to deal with the request unless it is clear that the

* 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 對個人資料之蒐集、處理、利用任一行為，皆統稱為「processing」。為與我國個人資料保護法中之「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」。

request is made under other rules than data protection rules.
然而，當事人毋須提出事由即可請求行使近用權，控管者亦毋須分析該請求是否確實有助於當事人查驗相關運用之合法性或行使其他權利。除非該請求顯然係依據資料保護規定以外之其他規定所提出，控管者必須受理該請求。

The right of access includes three different components:
近用權包含三個不同面向：

- Confirmation as to whether data about the person is processed or not,
  確認個人資料是否已被運用；
- Access to this personal data and
  近用該等個人資料；及
- Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.
  近用關於運用之資訊，如目的、資料類別及接收方、運用期間、當事人權利及若移轉至第三國之適當保護措施等。

General considerations on the assessment of the data subject's request
評估當事人請求之一般考量

When analysing the content of the request, the controller must assess whether the request concerns personal data of the individual making the request, whether the request falls within the scope of Art. 15 and whether there are other, more specific, provisions that regulate access in a certain sector. It must also assess whether the request refers to all or only parts of the data processed about the data subject.
於分析請求內容時，控管者必須評估該請求是否涉及提出請求人之個人資料，該請求是否屬於第 15 條範圍，及特定產業之近用是否受其他更具體條款所規範。控管者亦必須評估該請求是否涉及當事人全部或一部資料之運用。

There are no specific requirements on the format of a request. The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject. However, the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller. The controller is not obliged to act on requests that are sent to completely random, or apparently incorrect, addresses.
提出請求之格式並無具體規範。控管者應提供適當、方便使用，且當事人

可輕易使用的聯絡管道，惟不應要求當事人使用該等特定管道，而應允許當事人將請求發送予控管者之官方聯絡窗口。對於發送至完全隨機或明顯錯誤地址處之請求，控管者均無義務受理。

Where the controller is not able to identify data that refers to the data subject, it shall inform the data subject about this and may refuse to give access unless the data subject provides additional information that enables identification. Furthermore, if the controller has doubts about whether the data subject is who they claim to be, the controller must request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.
控管者若無法識別當事人之相關資料，控管者應通知當事人，且得拒絕該當事人之近用權請求，除非該當事人提供識別其身分之額外資訊。此外，若控管者對當事人所據稱之身分有疑慮，控管者必須要求當事人提供其他資訊以確認其身分。對額外資訊之要求必須與所運用之資料類型、可能發生之損害等符合比例，以避免過度蒐集資料。

Scope of the right of access
近用權之範圍

The scope of the right of access is determined by the scope of the concept of personal data as defined in Art. 4(1) GDPR. Aside from basic personal data like name, address, phone number etc. a broad variety of data may fall within this definition like medical findings, history of purchases, creditworthiness indicators, activity logs, search activities etc. Personal data which have undergone pseudonymisation are still personal data as opposed to anonymised data. The right of access refers to personal data concerning the person making the request. This should not be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages.
近用權之範圍係由 GDPR 第 4 條第 1 項所定義個人資料概念之範圍所決定。除基本個人資料（如姓名、地址、電話號碼等）外，其他廣泛類型之資料均可能屬此定義範圍，如醫療結果、購買紀錄、信用指標、活動紀錄、搜尋活動等。經過假名化處理的個人資料仍然屬個人資料，與匿名化資料相反。近用權係指與提出請求之當事人相關的個人資料。近用權之解釋不應被過度限縮，近用權亦得包括可能涉及他人的資料，例如涉及往來訊息的通訊紀錄。

In addition to providing access to the personal data, the controller has to provide

additional information about the processing and on data subjects' rights. Such information can be based on what is already compiled in the controller's record of processing activities (Art. 30) and the privacy notice (Art. 13 and 14). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request.
除提供個人資料之近用外，控管者必須提供關於運用及當事人權利之額外資訊。該等資訊得以控管者之運用作業紀錄（第 30 條）及隱私權通知（第 13 及 14 條）中已彙編之內容為基礎。然而，該等一般資訊可能需先更新至該請求之時間點，或就提出請求之當事人進行特別調整以反映對其所做之運用作業。

How to provide access
如何提供近用

The ways to provide access may vary depending on the amount of data and the complexity of the processing that is carried out. Unless explicitly stated otherwise, the request should be understood as referring to *all* personal data concerning the data subject and the controller may ask the data subject to specify the request if they process a large amount of data.
提供近用之方式可能因資料量及所做運用之複雜性而有所不同。除非另有明確說明，該請求應被理解為係指該當事人之*所有*個人資料，控管者若運用大量資料，則得要求當事人具體說明其請求。

The controller will have to search for personal data throughout all IT systems and non-IT filing systems based on search criteria that mirrors the way in which the information is structured, for example name and customer number. The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The more precise requirements in this regard depend on the circumstances of the data processing as well as the data subject's ability to grasp and comprehend the communication (for example taking into account that the data subject is a child or a person with special needs). If the data consists of codes or other "raw data", these may have to be explained in order to make sense to the data subject.
控管者必須依據反映資訊結構方式之搜尋標準，於所有資訊科技（IT）系統及非資訊科技（non-IT）檔案系統中搜尋個人資料，例如姓名及客戶號碼。資料之交流及其他關於運用之資訊，必須以簡明、透明、可理解及易近用之形式提供，並使用清晰及簡明之語言。這方面更精確的要求取決於資料運用之情況及當事人掌握及理解訊息的能力（例如，考量當事人為兒

童或有特殊需求之人）。若資料係由代碼或其他「原始資料」組成，則可能必須就其提供說明，使當事人得以理解該等資料。

The main modality for providing access is to provide the data subject with a copy of their data but other modalities (such as oral information and on site access) can be foreseen if the data subject requests it. The data can be sent by e-mail, provided that all necessary safeguards are applied taken into consideration, for example, the nature of the data, or in other ways, for example a self-service tool.
提供近用的主要方式是向當事人提供其資料之複製本，但若當事人要求，亦可透過其他方式（如口頭資訊及現場近用）提供。資料得透過電子郵件（惟必須在考量資料性質等因素後採取所有必要之保護措施）或其他方式（例如使用自助服務工具）提供。

Sometimes, when the amount of data is very vast and it would be difficult for the data subject to comprehend the information if given all in one bulk – especially in the online context - the most appropriate measure could be a layered approach. Providing information in different layers may facilitate the data subject's understanding of the data. The controller must be able to demonstrate that the layered approach has an added value for the data subject and all layers should be provided at the same time if the data subject requests it.
當資料量非常龐大時，若一次提供所有資訊，當事人會很難理解該等資訊（特別是透過線上提供的情況下），最適當的方式可能是分層提供。分層提供資訊可提升當事人對資料之理解。控管者必須能夠證明分層方法可對當事人提供附加價值，若當事人要求，所有層級資訊均應該同時提供。

The copy of the data and the additional information should be provided in a permanent form such as written text, which could be in a commonly used electronic form, so that the data subject can easily download it. The data can be given in a transcript or a compiled form as long as all the information is included and this does not alter or change the content of the information.
資料及額外資訊之複製本應以書面文本等永久形式提供，得以常用電子形式提供，使當事人易於下載。資料得以謄本或彙編之形式提供，但前提為其中應包含所有資訊，且資訊內容無任何替換或變更。

The request must be fulfilled as soon as possible and in any event within one month of receipt of the request. This can be extended by two further months where necessary, taking into account the complexity and number of the request. The data subject then has to be informed about the reason for the delay. The controller must implement necessary measures to deal with requests as soon as possible and adapt these measures to the circumstances of the processing. Where data is stored only

for a very short period, there must be measures to guarantee that a request for access can be fulfilled without the data being erased while the request is being dealt with. Where a large amount of data is processed, the controller will have to put in place routines and mechanisms that are adapted to the complexity of the processing.
請求必須盡快滿足，且無論如何應於收到請求後一個月內處理完成。考量到請求之複雜性及數量，必要時得再延長兩個月，且當事人必須被告知延遲的原因。控管者必須實施必要措施以盡快處理請求，並依據運用之情況實施相應措施。若資料僅被短期儲存，必須有措施可保證在處理請求時，近用權請求可獲得滿足，且相關資料不會被刪除。於運用大量資料的情況下，控管者應實施與運用之複雜性相應之流程與機制。

The assessment of the request should reflect the situation at the moment when the request was received by the controller. Even data that may be incorrect or unlawfully processed will have to be provided. Data that has already been deleted, for example in accordance with a retention policy, and therefore is no longer available to the controller does not have to be provided.
針對請求所作之評估應反映控管者收到請求時之情況。即使資料可能有不正確或非法運用的情況，仍必須提供資料。若資料已依據保留政策等原因而被刪除，控管者因此已不再持有該等資料，則毋須提供。

Limits and restrictions
限縮及限制

The GDPR allows for certain limitations of the right of access. There are no further exemptions or derogations. The right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject's request.
GDPR 允許對近用權設定部分限制，除此之外無其他豁免或例外。就控管者為滿足當事人之近用權請求所做的努力而言，並不適用一般比例性保留原則。

According to Art. 15(4) the right to obtain a copy shall not adversely affect the rights and freedoms of others. The EDPB is of the opinion that these rights must be taken into consideration not only when granting access by providing a copy, but also, if access to data is provided by other means (on-site access for example). Art. 15(4) is not, however, applicable to the additional information on the processing as stated in Art. 15(1) lit. a.-h. The controller must be able to demonstrate that the rights or freedoms of others would be adversely affected in the concrete situation. Applying Art. 15(4) should not result in refusing the data subject's request

altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.
依據第 15 條第 4 項，取得複製本之權利不得對他人之權利及自由產生不利影響。歐盟個人資料保護委員會（下稱「EDPB」）認為，該等權利不僅在透過提供複製本予以近用時必須予以考量，若透過其他方式（例如現場近用）提供近用資料，亦必須予以考量。然而，第 15 條第 4 項不適用第 15 條第 1 項第 a-h 款所定關於運用之額外資訊。控管者必須能夠證明他人之權利或自由在具體情況下會受到不利影響。第 15 條第 4 項之適用不應造成完全拒絕當事人之請求，而是僅應將可能對他人權利及自由產生不利影響之部分資料進行保留或使其無法識別。

Art. 12(5) allows controllers to reject requests that are manifestly unfounded or excessive, or to charge a reasonable fee for such requests. These concepts have to be interpreted narrowly. Since there are very few prerequisites regarding access requests, the scope of considering a request as manifestly unfounded is rather limited. Excessive requests depend on the specifics of the sector in which the controller operates. The more often changes occur in the controller's data base, the more often the data subject may be permitted to request access without it being excessive. Instead of refusing access, the controller may decide to charge a fee from the data subject. This would only be relevant in the case of excessive requests in order to cover the administrative costs that such requests may cause. The controller must be able to demonstrate the manifestly unfounded or excessive character of a request.
第 12 條第 5 項允許控管者拒絕顯無理由或過度之請求，或對該等請求收取合理費用。此概念必須做狹義解釋。因請求近用權之前提條件非常少，因此認定請求屬顯無理由的範圍相當有限。請求是否屬過度則取決於控管者所處產業之具體情況。控管者之資料庫進行變更的頻率越高，當事人即可越頻繁提出請求，而不被認定屬過度。在過度請求的情況下，控管者亦得決定向當事人收取一定費用，而不拒絕近用，以支付該等請求可能產生的行政成本。控管者必須能夠證明請求屬顯無理由或過度。

Restrictions of the right of access may also exist in Member States' national law as per Art. 23 GDPR and the derogations therein. Controllers who intend to rely on such restrictions must carefully check the requirements of the national provisions and take note of any specific conditions that may apply. Such conditions may be that the right of access is only temporarily delayed or that the restriction only applies to certain categories of data.
依據 GDPR 第 23 條及其中之例外規則，會員國之國家法規亦得就近用權設定限制。擬採用此種限制之控管者必須審慎確認國家法律規範，並注意任

何可能適用之具體條件。該等條件可能包括，近用權請求僅得暫時延遲滿足，或限制僅適用特定類別之資料。

Table of contents
目錄

1 INTRODUCTION - GENERAL OBSERVATIONS 導言－一般性意見...13
2 AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES 近用權之目的，GDPR 第 15 條之架構及一般原則 17
2.1 Aim of the right of access 近用權之目的 17
2.2 Structure of Article 15 GDPR GDPR 第 15 條之架構....20
2.2.1 Defining the content of the right of access 界定近用權之內容....23
2.2.1.1 Confirmation as to 'whether' or not personal data are being processed 確認「是否」正在運用個人資料 23
2.2.1.2 Access to the personal data being processed 近用被運用之個人資料 23
2.2.1.3 Information on the processing and on data subject rights 關於運用及當事人權利之資訊 24
2.2.2 Provisions on Modalities 關於近用方式之條款....25
2.2.2.1 Providing a copy 提供一份複製本 25
2.2.2.2 Providing further copies 提供更多複製本....27
2.2.2.3 Making the information available in a commonly used electronic form 以常用電子形式提供資訊 29
2.2.3 Possible limitation of the right of access 近用權可能之限制....30
2.3 General principles of the right of access 近用權之一般原則 30
2.3.1 Completeness of the information 資訊之完整性 31
2.3.2 Correctness of the information 資訊之正確性 35
2.3.3 Time reference point of the assessment 評估之時間參考點 36
2.3.4 Compliance with data security requirements 遵守資料安全規範...38
3 GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS 關於評估近用請求之一般考量 39
3.1 Introduction 導言 39
3.1.1 Analysis of the content of the request 對請求內容進行分析 40
3.1.2 Form of the request 請求之形式....45

3.1.3 Identification of the data subject and link between the personal data and the data subject 當事人之身分識別及個人資料與當事人間之連結 49
3.2 Issues with establishing the identity of the person making the request 確認提出請求之人身分的相關問題 50
3.3 Proportionality assessment regarding identification of the requesting person 關於識別請求人之比例性評估 54
3.4 Requests made via third parties / proxies 透過第三人/代理人提出之請求 60
3.4.1 Exercise of the right of access on behalf of children 代表兒童行使近用權 61
3.4.2 Exercising the right of access through portals / channels provided by a third party 透過第三人提供之入口網站/管道行使近用權 63
4 SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS 近用權之範圍及其涉及之個人資料及資訊 63
4.1 Definition of personal data 個人資料之定義 64
4.2 The personal data the right of access refers to 近用權所指之個人資料 72
4.2.1 “personal data concerning him or her”「關於他/她的個人資料」 72
4.2.2 Personal data which “are being processed”「正在被運用」的個人資料 76
4.2.3 The scope of a new request to access 新近用請求之範圍 77
4.3 Information on the processing and on data subject rights 關於運用及當事人權利之資訊 78
5 HOW CAN A CONTROLLER PROVIDE ACCESS? 控管者如何提供近用？ 86
5.1 How can the controller retrieve the requested data? 控管者如何檢索當事人請求的資料？ 86
5.2 Appropriate measures for providing access 提供近用之適當措施 88
5.2.1 Taking “appropriate measures” 採取「適當措施」 88
5.2.2 Different means to provide access 提供近用的不同方式 90

5.2.3 Providing access in a “concise, transparent, intelligible and easily accessible form using clear and plain language” 以「簡明、透明、可理解及易近用之形式，使用清晰及簡明之語言」提供近用 ..94
5.2.4 A vast amount of information necessitates specific requirements on how the information is provided 需提供大量資訊時之方式的具體規範 97
5.2.5 Format 格式 101
5.3 Timing for the provision of access 提供近用的時間點 105
6 LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS 近用權之限縮及限制 109
6.1 General remarks 一般性評論 109
6.2 Article 15 (4) GDPR GDPR 第 15 條第 4 項 110
6.3 Article 12(5) GDPR GDPR 第 12 條第 5 項 117
6.3.1 What does manifestly unfounded mean? 顯無理由之意義為何？ 118
6.3.2 What does excessive mean? 過度之意義為何？ 119
6.3.3 Consequences 後果 126
6.4 Possible restrictions in Union or Member States law based on Article 23 GDPR and derogations 基於 GDPR 第 23 條之歐盟或會員國法律之可能限制及減損情況 127
ANNEX – FLOWCHART 附錄－流程圖 130

The European Data Protection Board
歐盟個人資料保護委員會

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, (hereinafter "GDPR"),
依據歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過保護自然人關於個人資料運用*和自由流通的 2016/679/EU 規則第 70(1e)條規定，並廢除第 95/46/EC 號指令下稱(「GDPR」）；

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],
依據歐洲經濟區聯合委員會 2018 年 7 月 6 日第 154/2018 號決定修正的歐洲經濟區合約，特別是其附件 11 及第 37 號議定書[1]；

Having regard to Article 12 and Article 22 of its Rules of Procedure,
依據其議事規則第 12 條及第 22 條，

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a dedicated stakeholders event on data subject rights, in order to identify the challenges and interpretation issues faced in the application of the relevant provisions of the GDPR;
本指引之準備工作涉及利益關係人意見之蒐集，包括以書面形式蒐集，以及在針對當事人權利舉辦之利益關係人會議中進行蒐集，以瞭解於適用 GDPR 相關條款時會面臨的挑戰及解釋議題。

HAS ADOPTED THE FOLLOWING GUIDELINES
通過以下指引

1 INTRODUCTION - GENERAL OBSERVATIONS
導言－一般性意見

1. In today's society, personal data are processed by public and private entities, during many activities, for a wide array of purposes and in many different ways. Individuals may often be in a disadvantaged position in terms of understanding how their personal data are processed, including the technology used in the

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
本文件所稱「會員國」係指「歐洲經濟區會員國」。

particular case, whether it is by a private or a public entity. In order to protect personal data of natural persons in these situations, the GDPR has created a coherent and robust legal framework, generally applicable with regard to different types of processing, including specific provisions relating to data subject rights.
於現今社會，公共及私人實體均會於許多活動中，為廣泛目的透過許多不同的方式運用個人資料。當事人可能經常處於不利地位，無法瞭解其個人資料如何被運用，包括於特定情況下使用的技術，或其資料係由私人或公共實體所運用。為於該等情況下保護自然人之個人資料，GDPR 創建了具有一致性且堅實的法律框架，普遍適用於不同類型的資料運用作業，並包含與當事人權利相關之具體條文。

2. The right of access to personal data is one of the data subject rights provided for in Chapter III of the GDPR among other rights, such as for instance the right to rectification and erasure, the right to restriction of processing, the right to portability, the right to object or the right of not being subject to automated individual decision making, including profiling[2]. The right of access by the data subject is enshrined both in the Charter of Fundamental Rights of the EU (the Charter)[3] and in Art. 15 GDPR, where it is precisely formulated as the right of access to personal data and to other related information.
個資近用權是 GDPR 第三章所定當事人權利之一，其他當事人權利包括更正及刪除權、限制運用權、資料可攜權、拒絕權或不接受自動化個別決策（包括剖析）之權利[2]。當事人之近用權於歐盟基本權利憲章[3]及 GDPR 第 15 條中均有規範，將其精確界定為近用個人資料及其他相關資訊之權利。

3. Under the GDPR, the right of access consists of three components i.e. confirmation of whether or not personal data are processed, access to it, and information about the processing itself. The data subject can also obtain a copy of the processed personal data, whereas this possibility is not an additional data subject right but the modality of providing access to the data. Thus, the right of access can be understood both as the possibility of the data subject to ask the controller if personal data about him or her are processed and as the possibility to access and to verify these data. The controller shall provide to the data subject, on the basis of his/her request, the information falling within the scope of Art. 15(1) and (2) GDPR.

---

[2] Art. 15 - 22 GDPR.
GDPR 第 15 至 22 條。

[3] Under Art. 8 para. 1 of the Charter of Fundamental Rights of the European Union Everyone has the right to the protection of personal data concerning him or her. Under Art. 8 para. 2 sentence 2, everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified. 依據歐盟基本權利憲章第 8 條第 1 項，所有人均有權保護其個人資料。依據歐盟基本權利憲章第 8 條第 2 項第 2 句，所有人均有權近用其已被蒐集之資料，並有權要求更正該等資料。

依據 GDPR，近用權包括三個面向，亦即，確認個人資料是否被運用、近用資料，及關於運用本身之資訊。當事人亦得取得被運用之個人資料的複製本，而此並非額外的當事人權利，而是提供資料近用的方式。因此，近用權可被理解為，當事人向控管者詢問關於其個人資料是否被運用，且近用及查驗該等資料之可能性。控管者應依據當事人之要求，向其提供屬於 GDPR 第 15 條第 1 項及第 2 項範圍之資料。

4. The exercise of the right of access is realised both in the framework of data protection law, in accordance with the objectives of data protection law, and more specifically, in the framework of "*fundamental rights and freedoms of natural persons and in* particular *their right to the protection of personal data*", as put forward by Art. 1(2) GDPR. The right of access is an important element of the whole system.
近用權之行使既是於資料保護法律之框架內實現，符合資料保護法律之目標，更具體而言，亦係如 GDPR 第 1 條第 2 項所定，於「*自然人之基本權利及自由，特別是其保護個人資料之權利*」的框架內實現。近用權為整個體系的重要元素之一。

5. The practical aim of the right of access is to enable the natural persons to have the control over their own personal data. In order to realise this goal effectively in practice, the GDPR is aiming to facilitate this exercise by number of guarantees enabling the data subject to exercise this right easily, without unnecessary constraints, at reasonable intervals and without excessive delay or expense. All this should lead to more effective enforcement of the right of access by data subject in the digital age.
近用權之實務目的為使自然人能夠控制其個人資料。為於實務上有效地實現此目標，GDPR 透過多項保護措施來促進此權利之行使，使當事人能夠以合理頻率輕易地行使此權利，毋須受不必要的限制，亦不會產生過度延遲或費用。於數位時代中，該等措施應能使當事人更有效地行使近用權。

6. With regards to the development of the right of access, as part of the data protection legal framework, it should be stressed that it has been an element of the European data protection system from its beginning. In comparison with Directive 95/46/EC, the standard of the data subject rights set out in the GDPR has been both refined and strengthened; this also applies to the right of access. As the modalities of the right of access are now specified more precisely, it is also more instructive from the point of legal certainty for both the data subject and the controller. Besides, the specific wording of Art. 15, and the precise deadline for the provision of data under Art. 12(3) GDPR, obliges the controller to be prepared for data subject inquiries by developing procedures for handling requests.

關於近用權之發展，作為資料保護法律框架之一部分，需強調者為，其自始即屬歐洲資料保護體系之要素。相較於第 95/46/EC 號指令，GDPR 所定當事人權利標準已獲得改善及強化，近用權亦如此。因近用權的行使方式現已有更精確規範，自法律確定性的角度來看，這能夠為當事人及控管者提供更多指引。此外，GDPR 第 15 條的具體文字及第 12 條第 3 項規定提供資料之確切截止日期，使控管者有義務透過訂定處理請求的程序以針對當事人請求做好準備。

7. The right of access should not be seen in isolation as it is closely linked with other provisions of the GDPR, in particular with data protection principles including the fairness and lawfulness of processing, the controller's transparency obligation and with other data subject rights provided for in Chapter III of the GDPR.
近用權不應獨立看待，因為它與 GDPR 其他條款密切相關，特別係與資料保護原則（包括運用之公平性及合法性）、控管者之透明化義務及 GDPR 第三章所定其他當事人權利密切相關。

8. In the framework of data subject rights, it is also important to stress the significance of Art.12 GDPR which lays down requirements for appropriate measures adopted by the controller in providing the information referred to in Art. 13 and 14 GDPR and the communications referred to in Art. 15-22 and 34 GDPR; these requirements generally specify the form, manner and time limit for the responses to the data subject, and in particular for any information addressed to the child.
於當事人權利之架構中，GDPR 第 12 條亦十分重要，該條規定控管者於提供 GDPR 第 13 條及第 14 條所定資訊及 GDPR 第 15-22 條及第 34 條所定通訊時採取適當措施之要求。該等要求一般均規範控管者於回覆當事人時所應採取之形式、方式、時限，特別是發送予兒童的資訊。

9. The EDPB considers it necessary to provide more precise guidance on how the right of access has to be implemented in different situations. These guidelines aim at analysing the various aspects of the right of access. More particularly, the section hereafter is meant to give a general overview and explanation of the content of the Art. itself whereas the subsequent sections provide deeper analysis of the most frequent practical questions and issues concerning the implementation of the right of access.
EDPB 認為有必要就近用權在不同情況下的行使方式提供更精確的指導。本指引之目的為分析近用權的各個面向。更具體而言，下一節旨在對該條款本身之內容進行整體概述及解釋，而後續章節則針對行使近用權最常見的實務問題及議題進行深入分析。

2 AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES
近用權之目的，GDPR 第 15 條之架構及一般原則

2.1 Aim of the right of access
近用權之目的

10. The right of access is thus designed to enable natural persons to have control over personal data relating to them in that it allows them, "*to be aware of, and verify, the lawfulness of the processing*"[4]. More specifically, the purpose of the right of access is to make it possible for the data subject to understand how their personal data is being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide the individual with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).
因此，近用權之目的係為使自然人得以控制與其相關之個人資料，因為近用權允許其「*知悉並確認運用之合法性*」[4]。更具體而言，近用權之目的係為使當事人能夠瞭解其個人資料之運用方式及運用之後果，並確認被運用資料之正確性，而毋須就其意圖提出說明。換言之，近用權旨在為當事人提供充分、透明且易近用之資料運用（無論所採用技術為何）資訊，並使其得以依據 GDPR 查驗特定運用作業的不同面向（如合法性、正確性）。

11. The interpretation of the GDPR provided in these guidelines is based on the CJEU case law which has been rendered so far. Taking into account the importance of the right of access, related case law can be expected to evolve significantly in future.
本指引所載之 GDPR 解釋均係以歐盟法院迄今作成之案例法為基礎。考量到近用權之重要性，相關案例法預計於未來將有重大發展。

12. In accordance with CJEU decisions[5], the right of access serves the purpose of guaranteeing the protection of the data subjects' right to privacy and data protection with regard to the processing of data relating to them [6] and may facilitate the exercise of their rights flowing from, for example, Art. 16 to 19, 21 to 22 and

---

4 Recital 63 GDPR.
GDPR 前言第 63 段。

5 CJEU, C-434/16 (Nowak) and joined cases C-141/12 and C-372/12 (YS and Others).
歐盟法院，C-434/16（Nowak 案）及合併案件 C-141/12 及 C-372/12（YS 及他人）。

6 CJEU, C-434/16, Nowak, para. 56.
歐盟法院，C-434/16（Nowak 案），第 56 段。

82 GDPR. However, the exercise of the right of access is an individual's right and not conditional upon the exercise of those other rights and the exercise of the other rights does not depend on the exercise of the right of access.
依據歐盟法院決定[5]，近用權旨在保障當事人於其相關資料運用方面之隱私權及資料保護[6]，並協助當事人行使相關權利，例如，GDPR 第 16 至 19、21 至 22 及 82 條。然而，近用權之行使屬個人權利，不以行使其他權利為先決條件，其他權利之行使亦不取決於是否行使近用權。

13. Given the broad aim of the right of access, the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting (see section 3 on the analysis of the request) and whether they hold personal data relating to that individual (see section 4). Therefore, for example, the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller[7].
有鑑於近用權之目的廣泛，控管者在評估行使近用權之請求時，不適合將近用權之目的作為行使近用權之前提條件來進行分析。因此，控管者不應針對當事人「為何」行使近用權進行評估，而僅應評估當事人有「哪些」請求（見第 3 節之請求分析）及其是否持有與該當事人相關之個人資料（見第 4 節）。因此，舉例而言，控管者不應以當事人所請求提供的資料，可能會在其與控管者間之解僱或商業糾紛時，用於法庭上為其抗辯之理由或主張，而拒絕提供近用[7]。

Example: An individual was dismissed by their employer. One week later, the individual decides to collect evidence to file an unfair dismissal lawsuit against their former employer. With that in mind, they write to the former employer requesting access to all personal data relating to them, as data subject, that the former employer, as controller, processes.
範例：當事人遭其雇主解僱。一週後，該當事人決定蒐集證據，對其前雇主提起不當解僱之訴。為此，當事人寫信予其前雇主，請求近用前雇

[7] However, this is without prejudice to any applicable national procedural rules adopted in accordance with Art. 23 GDPR, which determine for example the boundaries of the information to be provided to or exchanged between the parties to ongoing (court) proceedings and other ongoing (legal) claims or causes of action arising in the context of that legal relationship.
然而，這並不影響依據 GDPR 第 23 條通過之任何適用之國家程序規則，例如，規範繫屬中（法院）訴訟程序及其他繫屬中（法律）請求或於該等法律關係中所產生請求權之各方當事人可提供或交換資訊範圍的規則。

主作為控管者所運用與該當事人相關的所有個人資料。

The controller shall not assess the intention of the data subject, and the data subject does not need to provide the controller with the reason for their request. Therefore, if the request fulfils all other requirements (see section 2), the controller needs to comply with the request, unless the request proves to be manifestly unfounded or excessive in accordance with art. 12 (5) of the GDPR (see section 6.3), which the controller is required to demonstrate.

控管者不應就當事人之意圖進行評估，當事人亦毋須向控管者說明其提出請求的事由。因此，若該請求符合所有其他要件（見第 2 節），控管者即須遵從該請求，除非依據 GDPR 第 12 條第 5 項（見第 6.3 節），該請求經證明為顯無理由或過度（應由控管者負責證明）。

Variation 1: The data subject exercises the right of access with regard to the personal data relating to them during the course of the lawsuit. However, the national law of the Member State, which governs the employment relation between the controller and the data subject, contains certain provisions that limit the scope of information to be provided to or exchanged between parties to ongoing or prospective legal proceedings, which are applicable to the unfair dismissal lawsuit that the data subject filed. In this context and provided that, these national provisions comply with the requirements posed by Art. 23 GDPR[8], the data subject is not entitled to receive more information from the controller than is prescribed by the national law provisions of the Member State governing the information exchange between parties to legal disputes.

例外 1：當事人於訴訟過程中就與其相關之個人資料行使近用權。然而，管轄控管者及當事人僱傭關係之會員國國家法規包含特定條款，限制繫屬中或即將開展法律程序之各方當事人提供或交換資訊之範圍，該等條款適用當事人所提不當解僱之訴。於此情況下，只要該等國家法規符合 GDPR 第 23 條之規範[8]，當事人得自控管者處取得的資料，即僅限於會員國國家法規就法律糾紛各方當事人間資訊交流所設範圍。

14. Although the aim of the right of access is broad, the CJEU illustrated also the limits of the remit of data protection law and the right of access. For instance, the CJEU found that the objective of the right of access guaranteed by EU data protection law is to be distinguished from that of the right of access to public documents established by EU and national legislation, the latter aiming at, "the greatest

[8] EDPB Guidelines 10/2020 on restrictions under article 23 GDPR, version for public consultation, 18 December
EDPB 關於 GDPR 第 23 條下限制之指引 10/2020，為徵詢公眾意見版本，12 月 8 日

possible transparency of the decision-making process of the public authorities and to promote good administrative practices"[9], an objective not sought by data protection law. The CJEU concluded that the right of access to personal data applies irrespective of whether a different kind of right of access with a different aim applies, such as in the context of an examination procedure.
雖然近用權之目的廣泛，但歐盟法院亦曾就資料保護法律及近用權之範圍限制提出說明。例如，歐盟法院認定，歐盟資料保護法律保障近用權之目標，應與歐盟及國家法規所載之公共文書近用權有所區別。後者的目的為「使公務機關之決策過程盡可能透明，並促進良好的行政實踐」[9]，此並非資料保護法律所追求的目標。歐盟法院所作結論為，無論是否適用具有不同目的且不同類型之近用權（例如於審查程序中行使），均適用個人資料之近用權。

2.2 Structure of Article 15 GDPR
GDPR 第 15 條之架構

15. In order to reply to a request for access and to ensure that none of its aspects might be disregarded, it is necessary first to understand the structure of Art. 15 and the constituent components of the right of access stipulated in this Article.
為回覆近用權請求並確保其各面向均不會遭忽視，首先有必要瞭解第 15 條之架構及該條所定近用權之構成要素。

16. Art. 15 can be broken down into eight different elements as listed in the table below:
第 15 條可細分為八項不同要素，如下表所列：

1.	Confirmation as to whether or not the controller is processing personal data concerning the requesting person 確認控管者是否正在運用請求人之個人資料	Art. 15(1), first half of the sentence 第 15 條第 1 項，前半句
2.	Access to the personal data concerning the requesting person 近用與請求人相關之個人資料	Art. 15(1), second half of the sentence (first part) 第 15 條第 1 項，後半句（第一部分）

[9] CJEU, Joined cases C-141/12 and C-372/12, YS and Others, para. 47.
歐盟法院，合併案件 C-141/12 及 C-372/12，YS 及他人，第 47 段。

3.	Access to the following information on the processing: 近用以下之運用相關資訊： (a) the purposes of the processing; 運用的目的； (b) the categories of personal data; 個人資料類別； (c) the recipients or categories of recipients; 接收方或接收方之類別； (d) the envisaged duration of the processing or the criteria for determining the duration; 設想之運用期限或判斷該期限之標準； (e) the existence of the rights to rectification, erasure, restriction of processing and objection to processing; 更正權、刪除權、限制運用權及拒絕運用權之存在； (f) the right to lodge a complaint with a supervisory authority; 向監管機關提出申訴之權利； (g) any available information on the source of the data, if not collected from the data subject; 於非直接向當事人蒐集資料的情況下，任何關於資料來源之可用資訊； (h) the existence of automated decision-making, including profiling and other information relating thereto. 自動化決策（包括剖析）之存在及其他相關資訊。	Art. 15(1), second half of the sentence (second part) 第 15 條第 1 項，後半句（第二部分）

4.	Information on safeguards pursuant to Art. 46 where the personal data are transferred to a third country or to an international organisation 當個人資料被移轉至第三國或國際組織時，依據第 46 條實施保護措施之資訊	Art. 15(2) 第 15 條第 2 項
5.	The obligation of the controller to provide a copy of the personal data undergoing processing 控管者提供其所運用個人資料之複製本的義務	Art. 15(3), first sentence 第 15 條第 3 項，第一句
6.	Charging of a reasonable fee by the controller based on administrative costs for any further copies requested by the data subject 控管者依據其行政成本就當事人請求提供額外複製本收取合理費用	Art.15(3), second sentence 第 15 條第 3 項，第二句
7.	Provision of information in electronic form 以電子形式提供資訊	Art. 15(3), third sentence 第 15 條第 3 項，第三句
8.	Taking into account the rights and freedoms of others 考量他人權利及自由	Art. 15(4) 第 15 條第 4 項

While all elements of Art. 15(1) and (2) together define the content of the right of access, Art.15(3) deals with the modalities of access, in addition to the general requirements set out in Art. 12. Art. 15(4) supplements the limits and restrictions that Art. 12(5) provides for all data subjects rights with a specific focus on rights and freedoms of others in the context of access.

雖然第 15 條第 1 項及第 2 項所定一切要件共同定義近用權內容，但除第 12 條所定一般要求外，第 15 條第 3 項亦就近用之方式有所規範。第 15 條第 4 項補充第 12 條第 5 項所定對所有當事人權利之限縮及限制，特別強調行使近用權時所涉他人權利及自由。

2.2.1 Defining the content of the right of access
界定近用權之內容

17. Art. 15(1) and (2) contain the following three aspects: first, the confirmation whether personal data of the requesting person are being processed, if yes, second, access to those data, and, third, information on the processing. They can be regarded as three different components which together build the right of access.
第 15 條第 1 項及第 2 項包含以下三個面向：第一，確認請求人之個人資料是否正在被運用，若是，第二，對該等資料之近用，及第三，與運用相關之資訊。前述面向得被視為三個不同組成部分，共同建構近用權。

2.2.1.1 Confirmation as to 'whether' or not personal data are being processed
確認「是否」正在運用個人資料

18. When making a request for access to personal data, the first thing that the data subjects need to know is whether or not the controller processes data concerning them. Consequently, this information constitutes the first component of the right of access under Art. 15(1). Where the controller does not process personal data relating to the data subject requesting the access, the information to be provided would be limited to confirming that no personal data relating to the data subject are being processed. Where the controller does process data relating to the data subject, the controller must confirm this fact to the data subject. This confirmation may be communicated separately, or it may be encompassed as part of the information on the personal data being processed (see below).
當事人於提出近用個人資料之要求時，首先必須確認控管者是否有運用其相關資料。因此，依據第 15 條第 1 項，該等資訊構成近用權之第一個面向。若控管者並未運用與請求近用之當事人相關的個人資料，所提供資訊將僅限於確認其並未運用與當事人相關之個人資料。若控管者確實有運用與當事人相關之資料，控管者必須向當事人確認此事實。此等確認得單獨傳達，亦得將其納入關於其運用個人資料之資訊中（見下文）。

2.2.1.2 Access to the personal data being processed
近用被運用之個人資料

19. Access to personal data is the second component of the right of access under Art. 15(1) and it constitutes the core of this right. It relates to the notion of personal data as defined by Art. 4(1) GDPR. Aside from basic personal data like name and address, an unlimited variety of data may fall within this definition, provided that they fall under the material scope of the GDPR, notably with regards to the way in which there are processed (Art. 2 GDPR). Access to personal data hereby means access to the actual personal data themselves, not only a general description of the

data nor a mere reference to the categories of personal data processed by the controller. If no limits or restrictions apply[10], data subjects are entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request (see para. 35). The obligation to provide access to the data does not depend on the type or source of those data. It applies to its full extent even in cases where the requesting person had initially provided the controller with the data, because its aim is to let the data subject know about the actual processing of those data by the controller. The scope of personal data under Art. 15 is explained in detail in sec. 4.1 and 4.2.

近用個人資料為第 15 條第 1 項所定近用權之第二個面向，構成此權利之核心，並與 GDPR 第 4 條第 1 項所定義之個人資料概念相關。除姓名及地址等個人基本資料外，只要屬於 GDPR 之實質範圍，特別是在運用方式上，各類資料均可能屬此定義範圍（GDPR 第 2 條）。近用個人資料於此係指實際近用個人資料本身，而非僅係個人資料之一般敘述，亦非僅係控管者所運用個人資料之類別。若不適用任何限制或拘束 [10]，則依其請求範圍，當事人有權對其相關資料之全部或一部進行近用（見第 35 條）。提供近用資料之義務並非依據該等資料之類型或來源。即使該等資料係由請求人直接向控管者提供，亦完全適用，因為其目的係為讓當事人知悉控管者對該等資料之實際運用情況。第 15 條所定個人資料之範圍於第 4.1 段及 4.2 段有詳細說明。

2.2.1.3 Information on the processing and on data subject rights
關於運用及當事人權利之資訊

20. The third component of the right of access is the information on the processing and on data subject rights that the controller has to provide under Art. 15(1)(a) to (h) and 15(2). Such information could be based on text taken, for example, from the privacy notice of the controller[11] or from the controller's record of processing activities referred to in Art. 30 GDPR, but may have to be updated and tailored to the data subject making the request. The content and degree of specification of the information is further elaborated in section 4.3.

近用權之第三個面向為控管者依據第 15 條第 1 項第 a-h 款及第 15 條第 2 項必須提供關於運用及當事人權利之資訊。該等資訊得擷取自例如控管者隱

[10] See section 6 of these Guidelines.
見本指引第 6 段。

[11] See for information on this Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").
關於第 29 條工作小組之資訊，見第 WP260 號指引修訂一版，2018 年 4 月 11 日，第 2016/679 號規則下之透明化指引－經 EDPB 認可（下稱「第 29 條工作小組透明化指引（經 EDPB 認可）」）。

私權通知之文字[11]，或自控管者之運用作業紀錄中摘取（如 GDPR 第 30 條所述），惟可能必須進行更新並針對提出請求之當事人進行調整。資訊之內容及具體程度將於第 4.3 節進一步說明。

2.2.2 Provisions on Modalities
關於近用方式之條款

21. Art. 15(3) supplements the requirements for the modalities of the reply to access requests laid down in Art.12 GDPR by some specifications in context of access requests.
第 15 條第 3 項對 GDPR 第 12 條所定近用請求之回覆方式規範進行補充，於近用請求之脈絡下提供相關說明。

2.2.2.1 Providing a copy
提供一份複製本

22. Under the first sentence of Art. 15(3) GDPR, the controller shall provide a free copy of the personal data which the processing relates to. The copy therefore refers only to the second component of the right of access («access to the personal data processed», see above). The controller must ensure that the first copy is free of charge, even where it considers the cost of reproduction to be high (example: the cost of providing a copy of the recording of a telephone conversation).
依據 GDPR 第 15 條第 3 項之第一句，控管者應免費提供一份被運用個人資料之複製本。因此，該複製本僅係指近用權的第二項組成部分（亦即「近用被運用之個人資料」，見上文）。控管者必須確保第一份複製本為免費提供，即使認為複製費用很高亦然（例如：提供電話錄音複製本之費用）。

23. The obligation to provide a copy is not to be understood as an additional right of the data subject, but as modality of providing access to the data. It strengthens the right of access to the data[12] and helps to interpret this right because it makes clear, that access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data. At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents (see section 5, para. 150). More generally speaking, there is no additional information to be given to the data subject upon providing a copy: the scope of the information to be contained in the copy is the scope of the access to the data under 15(1) (second

[12] The obligation to provide a copy was not mentioned in the Data Protection Directive 95/46/EC.
資料保護指令 95/46/EC 中沒有提到提供複製本之義務。

component of the right of access as referred to above, see para. 19).
提供複製本之義務不應被理解為當事人之額外權利，而應被理解為提供資料近用的方式；其強化資料之近用權 [12]，並有助於解釋這項權利，因為其清楚表明，第 15 條第 1 項下之資料近用包括所有資料之相關完整資訊，而不應被理解為僅提供相關資料之摘要。同時，提供複製本之義務並非為擴大近用權之範圍：其（僅）係指正在被運用之個人資料的複製本，而不必然係原始文件之複製本（見第 5 節，第 150 段）。更廣泛而言，於提供複製本時，毋須提供額外資訊予當事人：複製本所包含資訊之範圍係第 15 條第 1 項所定之資料近用範圍（上文所稱近用權第二個組成部分，見第 19 段）。

24. In light of the above, if access to the data in the sense of Art. 15(1) is given by providing a copy, the obligation to provide a copy mentioned under 15(3) is complied with. The obligation to provide a copy serves the objectives of the right of access to allow the data subject to be aware of, and verify the lawfulness of the processing (Recital 63). To achieve these objectives, the data subject will in most cases need to see the information not only temporarily. Therefore, the data subject will need to get access to the information by receiving a copy of the personal data.
綜上所述，若第 15 條第 1 項意義上之資料近用是透過提供複製本來進行，即已遵守第 15 條第 3 項所定提供複製本之義務。提供複製本之義務是為讓當事人知悉並查驗運用過程之合法性（前言第 63 段），這是近用權的目標。為實現該等目標，於大多數情況下，當事人閱覽資訊之需求並非暫時性質。因此，當事人需要透過取得個人資料之複製本來實現資訊之近用。

25. In view of the above, the notion of a copy has to be interpreted in a broad sense and includes the different kinds of access to personal data as long as it is complete (i.e. it includes all personal data requested) and possible for the data subject to keep. Thus, the requirement to provide a copy means, that the information on the personal data concerning the person who makes the request is provided to the data subject in a way which allows the data subject to retain all of the information and to come back to it.
基於上述，複製本之概念必須作廣義解釋，且包含對不同類型個人資料之近用，只要資料完整（亦即，包含所有要求之個人資料）且能夠讓當事人保留。因此，提供複製本之要求係指，應將提出請求人個人資料之相關資訊，以可使當事人保留所有資訊並重複閱覽的方式提供予當事人。

26. In spite of this broad understanding of a copy, and regarding that it is the main modality by which access should be provided, under some circumstances other modalities could be appropriate. Further explanations on copies and other modalities of providing access are given in section 5, in particular 5.2.2 and 5.2.5.

縱令複製本有上述廣泛解釋，且提供複製本為提供近用的主要方式，但於特定情況下，採取其他方式亦屬適當。關於複製本及提供近用的其他方式之進一步說明，請見第 5 節，特別是第 5.2.2 及 5.2.5 節。

2.2.2.2 Providing further copies
提供更多複製本

27. Art. 15(3), second sentence concerns situations where the data subject asks the controller for more than one copy, for example in case the first copy was lost or damaged or the data subject wants to pass on a copy to another person or a Supervisory Authority. On the basis that further copies must be provided by the controller upon request of the data subject, Art. 15 (3) rules, that for any further copy requested, the controller may charge a reasonable fee based on administrative costs (Art. 15 (3) sentence 2).
第 15 條第 3 項第二句涉及當事人要求控管者提供多於一份複製本的情況，例如第一份複製本滅失或損壞，或當事人欲將複製本提供予他人或監管機關的情況。於控管者必須依據當事人要求提供更多複製本之基礎上，第 15 條第 3 項規定，對於提供更多複製本之要求，控管者得依據行政成本收取合理費用（第 15 條第 3 項第二句）。

28. If the data subject asks for an additional copy after the first request was made, questions may arise on whether this should be regarded as a new request, or whether the data subject wants an additional copy of the data in the sense of Art. 15(3)(2), in which case a fee for an additional copy may be charged. The response to these questions depends solely on the content of the request: the request should be interpreted as asking for an additional copy, insofar as, in terms of time and scope, it concerns the same personal data set as the former request. If, however, the data subject aims to get information on the data processed at a different point in time or relating to a different range of data from the one initially requested, the right to obtain a free copy according to Art. 15(3), applies once again. This also is valid in cases where the data subject has made a first request shortly beforehand. A data subject may exercise its right of access through a subsequent request and obtain a free copy, unless the request is regarded as excessive under Art. 12(5) with the possibility of charging a reasonable fee in accordance with Art. 12(5)(a) (on excessive character of repetitive requests, see section 6).
若當事人於第一次請求後再請求提供額外複製本，可能會出現以下問題：這是否應被視為新的請求？或當事人是想要取得第 15 條第 3 項第二句意義上的資料額外複製本（於此情況下得收取額外複製本之費用）？該等問題的答案完全取決於請求內容：就時間及範圍而言，若請求涉及與先前請求相同之個人資料集，則該請求應被解釋為要求額外複製本。然而，若當事

人旨在取得於不同時間點運用資料之資訊，或與先前請求之資料範圍不同之資料資訊，則依據第 15 條第 3 項，取得免費複製本之權利應再次適用。這亦適用當事人於不久前曾提出第一次請求之情況。當事人得透過後續請求行使其近用權並取得免費複製本，除非該請求依據第 12 條第 5 項被認為屬過度，則得依據第 12 條第 5 項第 a 款收取合理費用（關於重複請求之過度特徵，見第 6 節）。

Example: A customer submits an access request to a trading company. One year after the reply of the company, the same customer makes a request for access under Art. 15 to the same company. Irrespective of whether there have been new business transactions or other contacts between the parties since the previous request, this second request is to be regarded as a new request. Even if no change in the data processing by the company occurred– which is not necessarily apparent to the data subject – the data subject has the right to get a free copy of the data.

範例：一家貿易公司的客戶向其提出一項近用權請求，同一客戶於該公司回覆請求一年後，再依據第 15 條向同一公司提出近用權請求。無論自上次請求後雙方是否有新的商業交易或其他往來，這第二次請求應被視為新的請求。即使該公司之資料運用沒有發生變更－這對當事人而言並非明顯可知之資訊－當事人有權利取得一份免費之資料複製本。

Variation 1: Even if the customer in the above cases places the new request for example only one week after the first request, this may, if it is not to be interpreted as a mere reminder of the first request, well be regarded as a new request under Art. 15(3), first sentence. Regarding the short interval and depending on the specific circumstances of the new request, its excessiveness according to Art. 12(5) is at issue (see section 6).

例外 1：於上述情境下，客戶即使是在第一次請求後一週就再提出新的請求（若該請求並非解讀為僅屬第一次請求之提醒），亦得被視為第 15 條第 3 項第一句所稱之新請求。關於時間間隔較短之新請求，取決於新請求之具體情況，會有第 12 條第 5 項所定之「過度」問題（見第 6 節）。

Variation 2: The request for a "new copy" of the information that had already been given in form of a copy in response to a previous request, for example in case that the customer lost the copy previously received, should, as a matter of course, be regarded as a request for an additional copy as it refers to the previous request in scope and time of the processing.

例外 2：若當事人要求提供先前已透過提供複製本形式回應請求之資訊的「新複製本」（例如，客戶遺失先前取得複製本的情況下），該請求應

被視為要求提供額外之複製本，因為其與先前請求之運用範圍與時間相同。

29. If the data subject repeats a first request for access on the grounds that the answer received was not complete or that no reasons had been given for the refusal, this request is not to be regarded as a new request, since it is merely a reminder of a first unsatisfied request.
若當事人以收到的回覆不完整或未說明拒絕提供複製本之理由為由，重複第一次之近用權請求，此請求不能被視為新的請求，因其僅為反映不滿意第一次請求之回覆。

30. Concerning the allocation of costs in cases of requests for an additional copy, Art. 15(3) establishes that the controller may charge a reasonable fee based on the administrative costs that are caused by the request. This means, that the administrative costs are a relevant criterion for fixing the level of the fee. At the same time, the fee should be appropriate, taking into account the importance of the right of access as a fundamental right of the data subject. The controller should not pass on overhead costs or other general expenses to the data subject, but should focus on the specific costs that where caused by providing the additional copy. When organising this process the controller should deploy its human and material resources efficiently in order to keep the costs of the copy low. In line with the accountability principle the controller should be able to demonstrate the adequacy of the fee.
關於申請額外複製本之費用，第 15 條第 3 項規定，控管者得依據因該申請產生之行政成本來收取合理費用。這表示行政成本為判斷費用水準之相關標準。同時，考量到近用權作為當事人基本權利之重要性，此費用金額應符合適當性。控管者不應將間接成本或其他一般費用轉嫁予當事人，而應將重點放在提供額外複製本所產生的具體費用上。於規劃此流程時，控管者應有效部署其人力及物力資源，以降低製作複製本之成本。依據課責性原則，控管者應證明其收費之適當性。

31. In case the controller decides to charge a fee, the controller should indicate the amount of costs it is planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request.
若控管者決定收取費用，控管者應說明其計畫向當事人收取之費用數額，俾以讓當事人有機會決定是否維持或撤回該請求。

2.2.2.3 Making the information available in a commonly used electronic form 以常用電子形式提供資訊

32. In the event of a request by electronic form means, information shall be provided by electronic means where possible and unless otherwise requested by the data subject (see Art. 12(3)). Art. 15(3), third sentence, complements this requirement in the context of access requests by stating, that the controller is in addition obliged to provide the answer in a commonly used electronic form, unless otherwise requested by the data subject. Art. 15(3) presupposes, that for controllers who are able to receive electronic requests it will be possible to provide the reply to the request in a commonly used electronic form (e.g. in PDF). This provision refers to all the information that needs to be provided in accordance with Art. 15(1) and (2). Therefore, if the data subject submits the request for access by electronic means, all information must be provided in a commonly used electronic form. Questions of format are further developed in section 5. The controller should, as always, deploy appropriate security measures, in particular when dealing with special category of personal data (see below, under 2.3.4).
於透過電子形式提出請求的情況下，除非當事人另有要求，應盡可能以電子形式提供資訊（見第 12 條第 3 項）。第 15 條第 3 項第三句補充近用權請求之此規範，指出控管者亦有義務以常用電子形式提供回覆，除非當事人另有要求。第 15 條第 3 項預設，能夠收受電子請求的控管者就應該能夠以常用電子形式（如 PDF 格式）回覆請求。此規定涵蓋依據第 15 條第 1 項及第 2 項必須提供的所有資訊。因此，若當事人以電子形式提交近用權請求，所有資訊必須以常用電子形式提供。關於格式之問題將於第 5 節中進一步說明。控管者同樣應採取適當之安全措施，特別是於運用特種個人資料時（見下文第 2.3.4 節）。

2.2.3 Possible limitation of the right of access
近用權可能之限制

33. Finally, in context of the right of access, a specific limitation is foreseen in Art. 15 (4). It states, that possible adverse effects on the rights and freedoms of others have to be considered. Questions as to the scope and the consequences of this limitation as well as to additional limits and restrictions set forth in Art. 12(5) or under Art. 23 GDPR are explained in section 6.
最後，第 15 條第 4 項就近用權設下具體限制，規定必須考量到對他人權利及自由可能產生的不利影響。關於此限制之範圍及後果，及 GDPR 第 12 條第 5 項或第 23 條所定其他限縮及限制之問題，將於第 6 節中說明。

2.3 General principles of the right of access
近用權之一般原則

34. When data subjects make a request for access to their data, in principle, the

information referred to in Art. 15 GDPR must always be provided in full. Accordingly, where the controller processes data relating to the data subject, the controller shall provide all the information referred to in Art. 15 (1) and, where applicable, the information referred to in Art. 15(2). The information must be complete, correct and up-to-date, corresponding as close as possible to the state of data processing at the time of receiving the request. Where two or more controllers process data jointly, the arrangement of the joint controllers regarding their respective responsibilities with regards to the exercise of data subject's rights, especially concerning the answer to access requests, does not affect the rights of the data subjects towards the controller to whom they address their request[13].
當事人提出近用其資料之請求時，原則上，GDPR 第 15 條所定資料必須隨時完整提供。因此，當控管者運用與當事人相關之資料時，控管者應提供第 15 條第 1 項所定之所有資訊，並於適用情況下提供第 15 條第 2 項所定資訊。該等資訊必須為完整、正確且最新資訊，且盡可能符合收到請求時之資料運用狀態。若有兩個以上之控管者共同運用資料，共同控管者就回覆當事人行使權利請求之責任分配，特別是就回覆近用權請求而言，並不影響當事人對其提出請求之控管者所享有的權利[13]。

2.3.1 Completeness of the information
資訊之完整性

35. Data subjects have the right to obtain, with the exceptions mentioned below, full disclosure of all data relating to them (for details on the scope, see section 4, para.). Unless explicitly requested otherwise by the data subject, a request to exercise the right of access shall be understood in general terms, encompassing all personal data concerning the data subject[14]. Limiting access to part of the information may be considered in the following cases:
當事人有權取得與其相關所有資料之完整揭露，惟下列例外情況除外（關於其範圍之詳細資訊，見第 4 節）。除非當事人明確提出其他要求，行使近用權之請求一般應被理解為包括所有關於該當事人之個人資料[14]。於下列情況下，得考量將近用範圍限縮於部分資訊：

a) The data subject has explicitly limited the request to a subset. In order to avoid providing incomplete information, the controller may consider this limitation of the data subject's request only if it can be certain that this interpretation

[13] EDPB Guidelines nr 07/2020 on the concepts of controller and processor in the GDPR, par. 162f.. Processors have to assist the controller, ibid, para. 129.
EDPB 關於 GDPR 控管者與受託運用者概念之指引 07/2020，第 162f 段。受託運用者必須協助控管者，同前註，第 129 段。

[14] For details please see section 5.2.3 below on the topic of layered approach.
詳情請見下文 5.2.3 節關於分層方法之討論。

corresponds to the wish of the data subject (for further details, see section 3.1.1, para. 51). In principle, the data subject shall not have to repeat the request for the transmission of all the data the data subject is entitled to obtain.
當事人已將其請求明確限縮於特定資料子集之情況。為避免提供不完整的資訊，控管者只有在確認此解釋符合當事人意旨時，始得考量配合當事人請求之限縮範圍（進一步資訊，見 3.1.1 節，第 51 段）。原則上，當事人應毋須重複請求傳輸其有權取得的資料。

b) In situations where the controller processes a large amount of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle. There may be ways to solve this problem, depending on the circumstances and the technical possibilities, for example by providing self-service tools in online contexts (see section 5 on the layered approach). If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). This exceptional situation may exist for example in case of a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches as well as in cases where the controller has been collecting data upon frequent activities of the data subject for years.
於控管者運用大量當事人資料的情況下，若當事人以非常籠統的措辭提出近用權請求，控管者可能會對當事人是否真的想要取得所有運用相關資訊或控管者所有分支機構業務活動之詳細資訊而有所疑問。若一開始並未向當事人提供可明確說明請求的工具，或當事人並未利用該等工具，就可能發生上列疑問。控管者就會面臨以下問題：該如何提供完整回覆，但同時避免向當事人提供過多當事人不感興趣且無法有效處理的資訊。此問題的可能解決辦法取決於當時的情況及技術可能性，例如於線上提供自助服務工具（見第 5 節分層方法）。若此等解決方案不適用，運用大量當事人資料之控管者得於提供資訊前要求當事人說明其請求所涉及之資料或運用（見 GDPR 前言第 63 段）。此等特殊情況可能存在下列情境：舉例而言，控管者為經營多領域業務活動的公司或有不同行政單位的公務機關，而當

事人之大量資料係由其分支機構進行運用，且控管者多年來持續蒐集當事人頻繁活動之資料。

Example 1: A public authority processes data on the data subject in a number of different departments concerning various contexts. File management and file keeping are partly processed by non-automated means and most of the data is only stored in paper files. Regarding the general wording of the request, the public authority doubts whether the data subject is aware of the extent of the request, especially the variety of processing operations that it would encompass, the amount of information and the number of pages that the data subject would receive.

範例 1：某公務機關於不同情境下透過多個不同部門運用當事人資料。檔案管理及檔案保存作業之其中一部分是透過非自動化方式辦理，大部分資料僅儲存於紙本檔案中。因當事人請求措辭籠統，該公務機關懷疑當事人是否確實瞭解其請求範圍，特別是其包含的各類運用作業，及當事人將收到的資訊量及文件頁數。

Example 2: A big insurance company receives a general access request by letter from a person who has been a customer for many years. Even though deletion periods are fully respected, the company actually processes a vast amount of data concerning the customer, because processing is still necessary to fulfil contractual obligations arising from the contractual relationship with the customer (including for example continuing obligations, communication on controversial issues with the customer and with third parties, …) or to comply with legal obligations (archived data that have to be stored for tax purposes, etc.). The insurance company may have doubts as to whether the request, that was made in very general terms, is really intended to encompass all kinds of those data. This may be especially problematic if the insurance company only has a postal address of the data subject and therefore has to send any information on paper. However, the same doubts may be relevant also when providing the information by other means.

範例 2：一家大型保險公司收到一名長期客戶透過郵件提出的近用權請求。雖然該公司完全依據相關期限刪除資料，但因該公司於履行與客戶契約關係所產生之契約義務（包括例如履行持續性義務、與客戶及第三人就有爭議的問題進行溝通等）或遵守法律義務（為稅務目的必須保存之存檔資料等），仍需運用大量客戶資料。因客戶請求之措辭非常籠統，該公司懷疑客戶是否真的想要取得包含所有類型的資料。若保險公司只有當事人的郵寄地址，因此必須以紙本方式發送資訊，就可能會特

別棘手；但在以其他方式提供資訊的情況下，也是會有相同的疑問。

If, in such cases, the controller decides to ask the data subject to specify the request, in order to fulfil its obligation to facilitate the exercise of the right of access (Art. 12(2) GDPR) the controller shall at the same time give meaningful information about all the processing operations concerning the data subject, like different branches of its activities, different databases etc.
於此情況下，若控管者決定要求當事人就其請求進行說明，以履行其促進近用權行使之義務（GDPR 第 12 條第 2 項），控管者應同時提供與當事人所有運用作業相關之有意義資訊，如其業務之不同部門、不同之資料庫等。

It is important to underline that the request for specification shall not aim at a limitation of the reply to the access request and shall not be used to hide any information on the data or the processing concerning the data subject. If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full.
需要強調者為，要求當事人就其請求進行說明的目的，並非為限制對近用權請求之回覆，亦不應被用來隱匿任何關於當事人資料或其運用之資訊。若被要求說明其請求範圍之當事人，確認其欲取得所關於他/她的個人資料，控管者當然必須提供全部資料。

In any case, the controller should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights (Art. 12(2) GDPR). Subject to these principles, the controller may await the answer of the data subject before providing additional data according to the data subject's wish, if the controller has provided the data subject with a clear overview of all processing operations that concern the data subject, including especially those that the data subject might not have expected, if the controller has also given access to all data that the data subject clearly aimed for, and if, furthermore, this information has been combined with clear indication of how to get access to the remaining parts of the processed data.
無論如何，控管者必須能夠證明，其處理請求的方式能夠使近用權發揮最廣泛的效果，且符合其促進行使當事人權利之義務（GDPR 第 12 條第 2 項）。以符合前述原則為前提，若控管者已向當事人提供當事人相關所有運用作業之清晰概述（特別是包括當事人可能未預期者），已就當事人明確請求之資訊提供所有相關資料之近用，且其回覆亦包含當事人近用其他被運用資料之方式，控管者得等待當事人回覆，再依據當事人意願提供額

外資訊。

c) Exceptions or restrictions to the right of access apply (see below in section 6). In such cases, the controller must carefully check to which parts of the information the exception relates to and provide all information that is not excluded by the exception. For example, confirmation of the processing of personal data itself (component 1) will mostly not be affected by the exception. As a result, information has to be provided about all the personal data and all the information referred to in Art. 15(1) and (2) that are not concerned by the exception or the restriction.
適用近用權之例外情況或限制之情況（見下文第 6 節）。於此情況下，控管者必須仔細確認例外情況涉及相關資訊的哪些部分，並提供所有不受例外情況所排除之資訊。例如，確認個人資料運用本身（第一個組成部分）大多不會受到例外情況所影響。因此，必須提供第 15 條第 1 項及第 2 項所定所有個人資料及所有不受例外情況或限制影響之資訊。

2.3.2 Correctness of the information
資訊之正確性

36. The information included in the copy of the personal data given to the data subject has to comprise the actual information or personal data held about the data subject. This includes the obligation to give information about data that are inaccurate or about data processing which is not or no longer lawful. The data subject may for example use the right of access to find out about the source of inaccurate data being circulated between different controllers. If the controller corrected inaccurate data before informing the data subject about it, the data subject would be deprived of this possibility. The same applies in case of unlawful processing. The possibility to know about unlawful processing concerning the data subject is one of the main purposes of the right of access. The obligation to inform about the unchanged state of processing is without prejudice to the obligation of the controller to end unlawful processing or to correct inaccurate data. Questions about the order in which those obligations should be fulfilled, are answered in the following.
提供當事人之個人資料複製本中所定資訊，必須包括控管者持有該當事人之實際資訊或個人資料，這包括提供關於資料不正確或資料運用不合法或不再合法之資訊的義務。例如，當事人得行使近用權來瞭解不正確資料於不同控管者間流通之來源。若控管者於告知當事人之前改正不正確資料，當事人將被剝奪此可能性，這同樣適用非法運用之情況。瞭解當事人資料之非法運用的可能性，為近用權的主要目的之一。控管者將其資料運用狀態不做任何更動地告知當事人之義務，不影響控管者終止非法運用或改正不正確資料之義務。關於履行該等義務之順序問題，將於下文中說明。

2.3.3 Time reference point of the assessment
評估之時間參考點

37. The assessment of the data being processed shall reflect as close as possible the situation when the controller receives the request and the response should cover all data available at that point in time. This means that the controller has to try to find out about all the data processing activities relating to the data subject without undue delay. Controllers are thus not required to provide personal data, which they processed in the past but which they no longer have at their disposal[15]. For instance, the controller may have deleted personal data in accordance with its data retention policy and/or statutory provisions and may thus no longer be able to provide the requested personal data. In this context, it should be recalled that the length of time for which the data are stored should be fixed in accordance with Art. 5(1)(e) GDPR, as any retention of data must be objectively justifiable.
針對正在運用之資料所進行的評估，應盡可能反映控管者收到請求時的情況，而回覆應涵蓋當時所有資料。這表示控管者必須試圖識別與當事人相關之所有資料運用作業，而不得無故遲延。因此，控管者毋須提供其於過去運用過但已不再持有的個人資料[15]。例如，控管者可能已依據其資料保留政策及/或法律規定刪除個人資料，因此可能不再能夠提供所請求的個人資料。於此情況下，應注意資料保存期間應依據 GDPR 第 5 條第 1 項第 e 款予以確定，因任何資料之保存均必須具有客觀合理性。

38. At the same time, the controller shall implement the necessary measures to facilitate the exercise of the right of access and to deal with such requests as soon as possible and before the data will have to be deleted. In the case of shorter retention periods than the timeframe to answer imposed by Art. 12(3) GDPR, the timing to answer the request should be adapted to the appropriate retention period in order to facilitate the exercise of the right of access and to avoid the permanent impossibility of providing access to the data processed at the moment of the request. In this respect, for example, the request for the right of access to personal data collected before entering a building for security purposes must be dealt with promptly before the personal data are erased.
同時，控管者應採取必要措施以促使近用權之行使，並於資料必須刪除前盡快處理該等請求。若保存期限短於 GDPR 第 12 條第 3 項所定回覆時限，回覆請求之時間應依據適當保存期間進行調整，以促使近用權之行使，並

[15] See, to that effect, further clarifications in section 4 of these guidelines, as well as in Court of Justice of the European Union, C-553/07, 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* on a right of access to information on the recipients or categories of recipient in respect of the past.
見本指引第 4 節之進一步說明，及歐盟法院 C-553/07 號判決，2009 年 5 月 7 日，*College van burgemeester en wethouders van Rotterdam 訴 M. E. E. Rijkeboer* 案，關於過去接收方或接收方類別資訊之近用權。

避免於當事人提出請求之時永遠無法提供被運用之資料。此方面之範例包括，為安全目的於進入建築物前蒐集之個人資料之近用權請求，必須於個人資料被刪除之前迅即處理。

39. Furthermore, the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access (see 2.3.2). If, in the course of processing the access request, the controller discovers inaccurate data or unlawful processing, the controller has to assess the state of the processing and to inform the data subject accordingly before complying with its other obligations. In its own interest, to avoid the need of further communication on this as well as to be compliant with the transparency principle, the controller should add information about the subsequent rectifications or deletions.
此外，控管者不應於回覆近用權請求時刪除或變更個人資料以故意逃避提供所請求個人資料之義務（見 2.3.2 節）。若於處理近用權請求之過程中，控管者發現資料不正確或非法運用，控管者必須評估運用之狀態，並於遵守其他義務之前通知當事人。為其自身利益，為避免進一步溝通需求，亦為符合透明化原則，控管者應進一步提供關於後續更改或刪除之資訊。

> **Example**: On the occasion of replying to an access request a controller realises, that an application of the data subject for a vacancy in the company of the controller has been stored beyond the retention period. In this case the controller cannot delete first and then reply to the data subject that no data (concerning the application) is processed. It has to give access first and delete the data afterwards. In order to prevent a subsequent request for erasure it would then be recommended to add information about the fact and time of the deletion.
> **範例**：於回覆近用權請求人時，控管者發現當事人對控管者公司職缺之申請資料已超過保存期限。於此情況下，控管者不能先刪除該等資料再回覆當事人無運用資料（與申請之相關資料）。控管者必須先向當事人提供近用，然後再刪除資料。為避免後續之刪除請求，建議同時向當事人提供關於刪除該等資料之事實與時間資訊。

In order to comply with the principle of transparency, controllers should inform the data subject as of the specific point in time of the processing to which the response of the controller refers. In some cases, for example in contexts of frequent communication activities, additional processing or modifications of the data may occur between this time reference point, at which the processing was assessed, and the response of the controller. If the controller is aware of such changes, it is recommended to include information about those changes as well as information

about additional processing necessary to reply to the request.
為遵守透明化原則，控管者應告知當事人控管者回覆所涉運用之具體時間點。於特定情況下，例如於頻繁溝通活動之情境下，在評估運用之時間參考點及控管者作出回覆之期間，可能會發生額外運用或資料變更。若控管者知悉該等變更，建議納入該等變更資訊，及為回覆請求所必須額外運用之資訊。

2.3.4 Compliance with data security requirements
遵守資料安全規範

40. Since communicating and making available personal data to the data subject is a processing operation, the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing (see Art. 5 (f), 24 and 32 GDPR). This applies independently of the modality in which access is provided. In case of non-electronic transmission of the data to the data subject, depending on the risks that are presented by the processing, the controller may consider using registered mail or, alternatively, to offer, but not oblige, the data subject to collect the file against signature directly from one of the controller's establishments. If, in line with Art. 12(1) and (3), information is provided by electronic means, the controller shall choose electronic means that comply with data security requirements. Also in case of providing a copy of the data in a commonly used electronic form (see Art 15(3)), the controller shall take into account data security requirements when choosing the means of how to transmit the electronic file to the data subject. This may include applying encryption, password protection etc.. In order to facilitate access to the encrypted data, the controller should also ensure that appropriate information is made available so that the data subject can access the requested information in clear. In cases where data security requirements would necessitate end-to-end encryption of electronic mails but the controller would only be able to send a normal e-mail, the controller will have to use other means, such as sending a USB-stick by (registered) letter post to the data subject.
因向當事人傳輸及提供個人資料亦屬一項運用作業，控管者有義務持續實施適當的技術性及組織性措施，以維持與運用風險相應之安全水準（見 GDPR 第 5 條第 f 款、第 24 及 32 條），無論提供近用之方式為何，此義務均有適用。在透過非電子形式將資料傳送予當事人的情況下，視運用所涉風險而定，控管者可考慮採用掛號信或提供（但非強制）當事人直接至控管者其中一個據點簽名取件之選項。若資訊係依據第 12 條第 1 項及第 3 項透過電子形式提供，控管者應採用符合資料安全規範之電子形式。另外，在透過常用電子形式提供資料複製本的情況下（見第 15 條第 3 項），控管者於選擇如何將電子檔案傳輸予當事人時，應考量資料安全規範。這可能

包括採用加密、密碼保護等措施。為便利當事人近用經加密之資料，控管者亦應確保提供適當資訊，俾使當事人能夠確實近用所請求之資訊。若資料安全規範要求就電子郵件進行端對端加密，但控管者僅能發送普通電子郵件，控管者必須使用其他方式提供資訊，例如透過（掛號）信件郵寄隨身碟給當事人。

3 GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS
關於評估近用請求之一般考量

3.1 Introduction
導言

41. When receiving requests for access to personal data, the controller must assess each request individually. The controller shall take into consideration, *inter alia*, the following issues, further developed in the following paragraphs: whether the request concerns personal data linked to the requesting person and who the requesting person is. This section aims to clarify what elements of the request for access the controller should take into account when carrying out its assessment and to discuss possible scenarios for such an assessment as well as its consequences. The controller, when assessing a request for access to personal data, shall also take into account, pursuant to Art. 12(2), the obligation to facilitate the exercise of the data subject rights, while keeping in mind the appropriate security of the personal data[16].
當收到近用個人資料之請求時，控管者必須對各請求進行個別評估。除其他事項外，控管者應*特別考量*以下問題（將於以下段落中進一步說明）：該請求是否涉及與請求人相關之個人資料？請求人是誰？本節旨在說明控管者在評估近用權請求時應考量哪些因素，並討論此等評估之可能情況及其後果。控管者於評估對個人資料之近用權請求時，亦應考量到依據第 12 條第 2 項規定，控管者有義務促進當事人權利之行使，同時應確保個人資料之適當安全[16]。

[16] The controller shall ensure appropriate security of the personal data, in accordance with the integrity and confidentiality principle (Art. 5(1)(f)), by implementing appropriate technical and organisational measures, as referred to in Art. 32 and elaborated in Art. 24. The controller shall be able to demonstrate that it ensures an adequate level of data protection, in line with the accountability principle (see also: Art. 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173 and EDPB Guidelines nr 07/2020 on the concepts of controller and processor in the GDPR).
控管者應依據完整性及保密原則（第 15 條第 1 項第 f 款），透過實施適當之技術性及組織性措施，確保個人資料之適當安全，如第 32 條及第 24 條所述。控管者應證明其依據課責原則確保資料保護之適當水準（另見，第 29 條工作小組第 3/2010 號關於課責性原則之意見（2010 年 7 月 13 日通過）（版本 00062/10/EN WP173）及 EDPB 關於 GDPR 控管者與受託運用者概念之指引 07/2020）。

42. Therefore, the controllers should be proactively ready to handle the requests for access to personal data. This means that the controller should be prepared to receive the request, assess it properly (this assessment is the subject of this section of the guidelines) and provide an appropriate reply without undue delay to the requesting person. The way the controllers will prepare themselves for the exercise of access requests should be adequate and proportionate and depend on the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, in accordance with Art. 24 GDPR. Depending on the particular circumstances, the controllers may for example in some cases be required to implement an appropriate procedure, the implementation of which should guarantee the security of the data without hindering the exercise of the data subject's rights.
因此，控管者應主動針對個人資料之近用請求進行備置，亦即控管者應該準備受理請求，對其進行適當評估（此等評估是為本指引中本章節的主題），並向請求人提供適當回覆，不得無故遲延。依據 GDPR 第 24 條，控管者應就近用權請求進行充分且符合比例的準備，並將運用之性質、範圍、背景及目的，與對自然人權利及自由之風險納入考量。視具體情況而定，例如在特定情況下，控管者可能會被要求實施適當之程序，而該程序之實施應於保證資料安全的同時也不妨礙當事人權利之行使。

3.1.1 Analysis of the content of the request
對請求內容進行分析

43. This issue can be more specifically assessed by asking the following questions.
此議題得透過下列問題來進行更具體之評估。

a) *Does the request concern personal data?*
請求是否涉及個人資料？

44. Under the GDPR, the scope of the request shall only cover personal data. Therefore, any request for information about other issues, including general information about the controller, its business models or its processing activities not related to personal data, is not to be considered as a request made pursuant to Art. 15 GDPR. Additionally, a request for information about anonymous data or data that does not concern the requesting person or the person on whose behalf the authorised person made the request, will not be within the scope of the right of access. This question will be analysed more in detail in section 4.
依據 GDPR，請求之範圍應僅限於個人資料。因此，任何關於其他議題之資訊請求，包括關於控管者、其商業模式或其運用作業等與個人資料無關之一般資訊，均不能被視為依據 GDPR 第 15 條提出之請求。此外，關於匿

名化資料或無涉請求人或提出請求之授權代理人所代表之人資料的資訊請求，均不屬近用權之範圍。此議題將於第 4 節進一步分析。

45. Unlike anonymous data (which are not personal data), pseudonymised data, which could be attributed to a natural person by the use of additional information, are personal data[17]. Thus, pseudonymised data that can be linked to a data subject - e.g. when the data subject provides the respective identifier allowing their identification, or when the controller is able to connect the data to the requesting person by its own means in accordance with Art 11(2) GDPR - are to be considered within the scope of the request[18].
與匿名化資料（非屬個人資料）不同，假名化資料（可透過使用額外資訊識別特定自然人）屬個人資料 [17]。因此，可與當事人連結之假名化資料（例如，當事人提供可識別其身分之相應識別碼時，或控管者能夠依據 GDPR 第 11 條第 2 項透過自己的方法將資料與請求人進行連結時）即應被視為屬於請求之範圍 [18]。

b) Does the request relate to the requesting person (or the person on whose behalf the authorised person makes the request)?
請求是否與請求人（或提出請求之授權代理人所代表之人）相關？

46. As a general rule, a request may only concern the data of the person making the request. Access to other people's data can only be requested subject to appropriate authorisation[19].
一般而言，一項請求僅能涉及提出請求人之資料。近用他人資料之請求僅得於已取得適當授權的情況下提出 [19]。

Example: Data subject X works as a department manager for a company that provides parking spaces for its managers at a company car park. Although data subject X has a permanent parking space, when the data subject arrives at the office for their second shift, this space is often already occupied by another car.

[17] See Recital 26 GDPR. Further explanations on the concepts of anonymous data and pseudonymised data can be found in WP29 Opinion 4/2007 on the concept of personal data, p. 18-21.
見 GDPR 前言第 26 段。關於匿名化資料及假名化資料概念之進一步解釋，可參考第 29 條工作小組關於個人資料概念之第 4/2007 號意見，第 18-21 頁。

[18] Art. 29 Working Party, WP242 rev.01, 5 April 2017, Guidelines on the right to data portability - endorsed by the EDPB (hereinafter "WP29 Guidelines on the right to data portability - endorsed by the EDPB"), p. 9.
第 29 條工作小組第 WP242 號指引，修訂一版，2017 年 4 月 5 日，關於資料可攜權之指引－經 EDPB 認可（下稱「第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）」），第 9 頁。

[19] See section 3.4 ("Requests made via third parties/proxies").
見第 3.4 節（下稱「透過第三人/代理人提出之請求」）。

Since this situation is repetitive, in order to identify the driver who unauthorised occupies its slot, the data subject asks the controller of the video surveillance system covering the office's parking lot area, for access to the personal data of this driver. In such a case, data subject X's request will not be a request for access to their personal data, as the request does not concern the requesting person's data, but the data of another person - and therefore it should not be considered a request under Art. 15 GDPR.

範例：當事人 X 於一家公司擔任部門主管，該公司於公司停車場為主管提供停車位。雖然當事人 X 有固定停車位，但當事人進辦公室輪班時，此車位通常已被另一輛車佔據。因為此情況重複發生，為識別未經授權佔用其車位的駕駛，當事人要求辦公室停車場監控系統的控管者提供該駕駛之個人資料。於此情況下，當事人 X 的請求並非近用其個人資料，由於該請求未涉及請求人之資料，而是他人資料，因此不應被視為 GDPR 第 15 條下之請求。

c) Do provisions, other than the GDPR, regulating access to a certain category of data apply?
除 GDPR 外，是否也適用其他規範特定類型資料近用之法規？

47. Data subjects are not required to specify the legal basis in their request. However, if the data subjects clarify that their request is based on sectoral legislation[20] or on national legislation regulating the specific issue of access to certain categories of data[21], and not on the GDPR, such a request shall be exercised by the controller in accordance with such sectoral or national rules. If the data subjects also request access to their data under Art. 15, and the controller has already provided data under the sectoral legislation, the controller should verify whether the obligations under the GDPR have been already fulfilled (i.e. all elements of Art. 15 have been already provided) or not (in that case additional elements have to be provided by the controller). Often, depending on the relevant national legislation, controllers may be required to provide separate replies, each dealing with the specific requirements set out by the different legislative acts. This is not to be confused with national or EU legislation setting out restrictions on the right of access which

[20] See WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 8, footnote 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*"
見第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）第 8 頁，註腳 15：「*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近用，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近用。*」

[21] Such as, for example, regulated access to medical records in some national legislation.
例如，某些國家法規對病歷之近用有所規範。

needs to be complied with when answering access requests.
當事人毋須於其請求中說明法律依據。然而，若當事人說明其請求依據為關於特定類別資料之具體近用議題的產業法規 [20] 或國家法規 [21]，而非基於GDPR，則控管者應依據該等產業或國家法規處理該要求。若當事人亦依據第 15 條請求近用其資料，而控管者已依據產業法規提供資料，控管者應確認其是否已履行 GDPR 下之義務（亦即，第 15 條之所有規定均已履行）（於未履行的情況下，控管者必須提供額外資料）。一般情況下，視相關國家法規而定，控管者可能被要求另行提出回覆，以分別處理不同法規所定具體規範。此與各國法規或歐盟法規針對近用權所設之限制（且控管者於回覆近用請求時必須遵守者）不應混為一談。

48. If the controller has doubts as to which right the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain the subject matter of the request. Such correspondence with the data subject shall not affect the duty of the controller to act without undue delay[22]. However, in case of doubts, if the controller asks the data subject for further explanation and receives no response, the controller should interpret, bearing in mind the obligation to facilitate the exercise of the person's right of access, the information contained in the first request and act on its basis. In accordance with the accountability principle, the controller may determine an appropriate timeframe during which the data subject may provide further explanations. When fixing such timeframe, the controller should leave enough time to comply with the request after it elapsed and therefore consider how much time is objectively necessary to compile and provide the requested data once the specification was provided (or not) by the data subject.
若控管者對當事人擬行使之權利有疑問，建議要求提出請求之當事人說明請求事項。與當事人進行此等溝通時，控管者仍有義務迅即採取行動，不得無故遲延 [22]。然而，於有疑問的情況下，若控管者要求當事人進一步說明但卻未得到回應，控管者應以第一次請求中所提供之資訊為基礎進行解釋及採取行動，惟仍應謹記其有義務促使當事人行使近用權。控管者得依據課責性原則判斷當事人得提供進一步說明之時限。於判斷該時限時，控管者應考量其於該時限屆滿後遵守請求所需之充分時間，並據此考量當事人在說明（或未說明）請求範圍後，編纂及提供所請求資料之客觀必要時間為何。

49. If the request is aimed at obtaining access under the GDPR, the existence of such specific legislation does not override the general application of the right of access, as provided by the GDPR. There might be restrictions set out by EU or national

[22] See further guidance on the timing in section 5.3.
見第 5.3 節中關於時間點之進一步指導。

law, when allowed by Art. 23 GDPR (see section 6.4).
若請求之目的係為依據 GDPR 取得近用，則依據 GDPR 規範，該等具體法規之存在並不能推翻近用權之一般適用。於 GDPR 第 23 條允許的情況下，歐盟或國家法規可能會訂定相關限制（見 6.4 節）。

d) Does the request fall within the scope of Article 15?
請求是否屬第 15 條範圍？

50. It should be noted that the GDPR does not introduce any formal requirements for persons requesting access to data. In order to make the access request, it is sufficient for the requesting persons to specify that they want to know what personal data concerning them the controller processes. Therefore, the controller cannot refuse to provide the data by referring to the lack of indication of the legal basis of the request, especially to the lack of a specific reference to the right of access or to the GDPR.
應注意者為，GDPR 並未對請求近用資料之人設定任何正式規範。若欲提出近用權請求，請求人僅需說明其欲知悉控管者運用哪些與其相關之個人資料。因此，控管者不能以請求人並未說明其請求之法律依據（特別是未具體提及近用權或 GDPR）而拒絕提供資料。

For example, in order to make a request, it would be sufficient for the requesting persons to indicate that:
例如，為提出請求，請求人僅需表明：

- they wish to obtain access to the personal data concerning them;
  其擬取得關於其個人資料之近用；
- they are exercising their right of access; or
  其正在行使其近用權；或
- they wish to know the information concerning them that the controller processes.
  其欲知悉控管者運用其相關資料之資訊。

It should be borne in mind that applicants may not be familiar with the intricacies of the GDPR and that it is advisable to be lenient towards persons exercising their right of access, in particular when it is exercised by minors. As indicated above, in case of any doubts it is recommended for the controller to ask the data subject making the request to specify the subject matter of the request.
應注意者為，因申請人可能不瞭解 GDPR 的複雜性，建議以寬容的態度對待行使近用權之人，特別是在未成年人欲行使近用權時。如上所述，在有

任何疑問的情況下，建議控管者要求提出請求之當事人說明其請求事宜。

e) Do the data subjects want to access all or parts of the information processed about them?
當事人是否想近用其被運用資料之全部或一部？

51. Additionally, the controller needs to assess whether the requests made by the requesting persons refer to all or parts of the information processed about them. Any limitation of the scope of a request to a specific provision of Art. 15 GDPR, made by the data subjects, must be clear and unambiguous. For example, if the data subjects require verbatim "information about the data processed in relation to them", the controller should assume that the data subjects intend to exercise their full right under Art. 15(1) – (2) GDPR. Such a request should not be interpreted as meaning that the data subjects wish to receive only the categories of personal data that are being processed and to waive their right to receive the information listed in Art. 15(1)(a) to (h). This would be different, for example, where the data subjects wish, with regard to data which they specify, to have access to the source or origin of the personal data or to the specified period of storage. In such a case the controller may limit its reply to the specific information requested.
此外，控管者需要評估申請人提出之請求係關於其被運用資料之全部或一部。若欲將當事人請求範圍限縮於 GDPR 第 15 條下之特定條款，必須有明確且非模稜兩可的依據。例如，若當事人明確要求提供「其被運用資料之相關資訊」，控管者應假設當事人擬行使其於 GDPR 第 15 條第 1 項及第 2 項下之全部權利。此要求不應被解釋為，當事人僅欲知悉其正在被運用之個人資料的類別，並拋棄其取得第 15 條第 1 項第 a-h 款所列資訊之權利；但若當事人就特定資料說明其欲瞭解該等資料之來源或出處或其保存期限，則有所不同；於此情況下，控管者得將其回覆限縮於所請求之具體資訊。

3.1.2 Form of the request
請求之形式

52. As noted previously, the GDPR does not impose any requirements on data subjects regarding the form of the request for access to the personal data. Therefore, there are in principle no requirements under the GDPR that the data subjects must observe when choosing a communication channel through which they enter into contact with the controller.
如前所述，GDPR 並未就請求近用個人資料之形式向當事人施加任何規範。因此，GDPR 原則上並未要求當事人必須透過特定聯絡管道與控管者聯繫。

53. The EDPB encourages the controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25, to enable the

data subject to make an effective request. Nevertheless, if the data subject makes a request using a communication channel provided by the controller[23], which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly (see the examples below). The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated (for example, in case the data subject sends the request to an employee who is on leave, an automatic message informing the data subject about an alternative communication channel for its request could be a reasonable effort).
EDPB 鼓勵控管者依據第 12 條第 2 項及第 25 條，提供最適當及最方便的聯絡管道，使當事人能夠提出有效請求。然而，若當事人使用由控管者提供之聯絡管道為請求 [23]，並非採用控管者標明應優先採用之管道，該請求於一般情況下仍應被視為有效，控管者應據以受理該請求（範例見下文）。控管者應行使最大合理努力，以促成當事人權利之行使（例如，若當事人將請求發送予正在休假的員工，則自動將替代的請求聯絡管道通知當事人，亦屬行使合理努力）。

54. It should be noted that the controller is not obliged to act on a request sent to a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights, if the controller has provided an appropriate communication channel, that can be used by the data subject.
應注意者為，若控管者已提供當事人得使用之適當聯絡管道，控管者無義務對發送至隨機或不正確，且非控管者直接提供的電子郵件（或實體）地址，或發送至任何明顯非受理當事人權利請求之聯絡管道的請求採取行動。

55. The controller is also not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel. However, if the data subject sends a request to the controller's employee who deals with the data subject's affairs on a daily basis (single contact of a customer, such as e.g. personal account manager), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it

[23] This may include, for example, communication data of the controller provided in its communications addressed directly to data subjects or contact data provided by the controller publicly, such as in the controller's privacy policy or other mandatory legal notices of the controller (e.g. owner or business contact information on a website).
例如，這可能包括控管者於直接發送予當事人之通訊中提供的聯絡資料或控管者公開提供的聯絡資料，如控管者之隱私權政策或其他具強制性之法律通知（例如，網站上提供所有人或業務窗口之資訊）。

can be redirected to the contact point and answered within the time limits provided for by the GDPR.
控管者亦無義務對發送至可能未涉及受理當事人權利請求之控管者員工（如司機、清潔人員等）電子郵件地址之請求採取行動。若控管者已明確向當事人提供適當聯絡管道，則該等請求將不視為有效。然而，若當事人向控管者日常負責處理當事人事務之員工發送請求（單一客戶聯絡人，例如：個人帳戶經理），則該聯繫不應被視為隨機，控管者應盡最大合理努力處理該等請求，將其轉介予適當聯絡窗口，並於 GDPR 規定時限內回覆。

56. Nevertheless, the EDPB recommends, as good practice, that controllers introduce, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests. In order to facilitate the exercise of data subjects' rights.
然而，EDPB 建議，良好的作法是，控管者於可行情況下應針對發送予無權受理當事人請求員工之請求，建立相關機制來改善員工間的內部溝通，以促使當事人權利之行使。

Example: Controller X provides, both on its website and in the privacy notice, two e-mail addresses - the general e-mail address of the controller: CONTACT@X.COM and the e-mail address of the controller's data protection contact point: QUERIES@X.COM. Additionally, controller X indicates on its website that in order to submit any inquiries or to make a request with regard to the processing of personal data, one shall contact the data protection contact point under the e-mail address provided. However, the data subject sends a request to the controller's general e-mail address: CONTACT@X.COM.
範例：控管者 X 於其網站及隱私權聲明中提供兩個電子郵件地址－控管者的一般電子郵件地址：CONTACT@X.COM；及控管者資料保護聯絡窗口的電子郵件地址：QUERIES@X.COM。此外，控管者 X 於其網站上表示，若欲提交任何詢問或提出關於個人資料運用之請求，應透過其所提供的電子郵件地址，聯繫資料保護聯絡窗口。然而，當事人仍將請求發送至控管者的一般電子郵件地址 CONTACT@X.COM。

In such a case, the controller should make all reasonable efforts, to make its services aware of the request, which was made through the general e-mail, so that it can be redirected to the data protection contact point and answered within the time limits provided for by the GDPR. Moreover, the controller is not entitled to extend the period for responding to a request, merely because the data subject has sent a request to the controller's general e-mail address, not the controller's data protection contact point e-mail address.

於此情況下，控管者應盡最大合理努力，使其服務人員知悉此透過一般電子郵件提出之請求，使其得以被轉介予資料保護聯絡窗口，並於 GDPR 規定時限內回覆。此外，控管者無權僅因當事人將請求發送至控管者之一般電子郵件地址，而非控管者之資料保護聯絡窗口電子郵件地址，而延長對該請求作出回覆的期限。

Example: Controller Y runs a network of fitness clubs. Controller Y indicates on its website and in the privacy notice for clients of the fitness club that in order to submit any inquiries or to make a request with regard to the processing of personal data, one shall contact the controller under the e-mail address: QUERIES@Y.COM. Nevertheless, the data subject sends a request to an e-mail address found in the changing room, where he found a notice that reads "If you are not satisfied with the cleanliness of the room, please contact us at: CLEANERS@Y.COM", which is the e-mail address of the cleaning staff employed by Y. The cleaning staff are obviously not involved in handling matters concerning the exercise of the rights of data subjects - customers of the fitness club. Although the e-mail address was available on the premises of the fitness club, the data subject could not reasonably expect that this was an appropriate contact address for such requests, since the website and the privacy notice clearly informed about the communication channel to be used for the exercise of data subjects' rights.

範例：控管者 Y 經營健身俱樂部網站。控管者 Y 於其網站上提供給健身俱樂部客戶的隱私權聲明中指出，若欲提出任何詢問或關於個人資料運用之請求，應透過電子郵件（QUERIES@Y.COM）聯絡控管者。然而，某當事人卻向他在更衣室看到的電子郵件地址發出請求，該當事人在更衣室看到的訊息寫著：「若您對更衣室的整潔度不滿意，請與我們聯絡：CLEANERS@Y.COM」；這是 Y 公司清潔人員的電子郵件地址。清潔人員顯然不參與處理當事人（健身俱樂部之客戶）行使權利之事宜。雖然該電子郵件地址於健身俱樂部場館內可見，但當事人無法合理期待這是提出此種請求之適當聯絡地址，因為網站及隱私權聲明中明確告知當事人行使權利的聯絡管道。

57. Date of receipt of the request by the controller triggers, as a rule, the one month period for the controller to provide information on action taken on a request, in accordance with Art. 12(3) (further guidance on timing is provided in section 5.3).

The EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one month period runs from day X to day Y.
依據第 12 條第 3 項，控管者收到請求的日期，原則上成為控管者需於一個月內提供其就該請求採取行動之相關資訊的起始日（關於此時限之進一步說明，見第 5.3 條）。EDPB 認為良好的做法為，控管者應以書面形式確認收到請求，例如透過發送電子郵件（或透過實體郵寄，如可行）予請求人，確認已收到其請求，及該一個月期間起始日分別為 X 日及 Y 日。

3.1.3 Identification of the data subject and link between the personal data and the data subject
當事人之身分識別及個人資料與當事人間之連結

58. In order to ensure the security of processing and minimize the risk of unauthorised disclosure of personal data, the controller must be able to identify the data subject, i.e. find out which data refer to the data subject, and confirm the identity of the person in case of doubts[24].
為確保運用之安全性，並盡可能減少未經授權揭露個人資料之風險，控管者必須能夠識別當事人，亦即，找出哪些資料與該當事人相關，並在有疑問的情況下確認該人身分[24]。

59. The GDPR does not impose any requirements regarding the methods for determining the identity of the data subject. However, Art. 11 and 12 indicate the conditions for the exercise of all the data subject rights, including the right of access to personal data.
GDPR 並未對識別當事人身分的方法提出任何規範。然而，第 11 條及第 12 條規定行使所有當事人權利（包括近用個人資料之權利）的條件。

60. It should be remembered that, as a rule, the controller cannot request more personal data than is necessary to enable this identification, and that the use of such information should be strictly limited to fulfilling the data subjects' request.
應注意者為，控管者原則上不得要求提供其他個人資料來協助其進行識別，且該等資訊僅得用於回覆當事人請求。

61. Art. 12(2) states that the controller shall not refuse to act on the request of the data subject to exercise his or her rights, unless the controller demonstrates that it is not

[24] See further considerations regarding the identification of a natural person in WP29 Opinion 4/2007 on the concept of personal data, paragraph III.3.
見第 29 條工作小組關於個人資料概念之第 4/2007 號意見中對自然人身分之進一步考量，第 III.3 段。

in a position to identify the data subject. In such circumstances, the data subject may, however, provide additional information enabling this identification (Art. 11(2)). In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification.
第 12 條第 2 項規定，控管者不得拒絕當事人行使其權利之請求，除非控管者可證明其無法識別當事人。於此情況下，當事人得提供額外資訊以協助識別（第 11 條第 2 項）。為使當事人提供識別其資料所必須的額外資訊，控管者應告知當事人該等必要額外資訊之性質。

62. If the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art. 12(6)).
若控管者對提出請求之自然人的身分有合理懷疑，控管者得要求提供必要之補充資訊，以確認當事人身分（第 12 條第 6 項）。

63. As indicated in the WP29 Guidelines on Data Portability endorsed by the EDPB, insofar as a digital communication channel already exists between the data subject and the controller and without prejudice to Art. 12(6) GDPR. The controllers must implement or re-use an authentication procedure in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR[25].
如第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）所述，若當事人及控管者之間已存在數位聯絡管道，於不影響 GDPR 第 12 條第 6 項的情況下，控管者必須實施或重新使用認證程序，以確定請求提供其個人資料或行使 GDPR 所授予權利之當事人身分[25]。

3.2 Issues with establishing the identity of the person making the request
確認提出請求之人身分的相關問題

64. The controller should act upon the requests of data subjects for exercising their individual rights, unless it can demonstrate - through a justification in line with the principle of accountability (Art. 5(2)) - that it is not in a position to identify the data subject (Art. 11). The controller is not obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with the request. However, it should not refuse to take such additional information (Recital 57).
控管者應依據當事人行使其個人權利之請求採取行動，除非其能提出符合

[25] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 14 頁。

課責性原則（第 5 條第 2 項）之理由證明其無法識別當事人（第 11 條）。控管者無義務僅為回覆請求而取得額外資訊來識別當事人。然而，控管者不應拒絕取得此等額外資訊（前言第 57 段）。

Example: X is the controller of the data processed in connection with the video surveillance of a building. In accordance with Art. 11(1), the controller is not obliged to identify all persons who have been registered by a security camera as a part of the monitoring (purpose not requiring identification). The controller receives a request for access to the personal data from the person who claims that to have been recorded by the controller's video surveillance. The controller's actions will depend on the additional information provided. If the requesting person indicates a particular day and time when the cameras may have recorded the event in question, it is likely that the controller will be able to provide such data (Art. 11(2)). However, if the request concerns e.g. a year of recordings, a controller who is unable to process such a large amount of data may refuse to take action not being in the position to identify the data subject (Art. 12(2)).

範例：X 為某建物監視器之被運用資料的控管者。依據第 11 條第 1 項，控管者無義務識別所有出現在安全監視用錄影畫面之人（其目的毋須識別當事人）。控管者收到據稱出現於控管者監視畫面之人提出的個人資料近用請求時，控管者的行動將取決於其所取得的額外資訊。若請求人提供該等畫面之錄製日期與時間，則控管者即可能可以提供該等資料（第 11 條第 2 項）。然而，若該請求涉及控管者無法處理之大量資料(如一年的錄影畫面)，則可能會拒絕採取行動，因其無法識別當事人（第 12 條第 2 項）。

65. In cases where the controller requests the provision of additional information necessary to confirm the identity of the data subject, the controller shall each time assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3). Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication). In general, the fact that the controller may request additional information to assess the data subject'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[26].
於控管者要求提供必要額外資訊以確認當事人身分的情況下，控管者每次均應評估哪些資訊可幫助其確認當事人身分，且於符合比例原則的情況下，亦可能向請求人提出額外問題，或要求當事人提供額外的身分識別要件（見 3.3 節）。該等額外資訊不應超過最初驗證（認證）當事人身分所必須之資訊。一般而言，控管者得要求提供額外資訊來評估當事人身分之事實，不應導致過度要求及蒐集不相關或不必要的個人資料來強化當事人及所請求個人資料間之連結[26]。

66. As a consequence, where information collected online is linked to pseudonyms or other unique identifiers, the controller can implement appropriate procedures enabling the requesting person to make a data access request and receive the data relating to them[27].
因此，若透過線上蒐集的資訊與假名或其他獨特識別碼有所連結，控管者可實施適當程序，使請求人能夠提出資料近用權請求，並取得與其相關之資料[27]。

> **Example**: The data subject Ms. X requests access to her data while speaking to a helpline consultant of an electricity company with which she has concluded a contract. The consultant, having doubts as to the identity of the person making the request, generates in the company's system a one-time unique code sent to the user's mobile phone number, provided when the account was set up, as part of the double verification system, which action should be considered proportionate in this case.
> **範例**：當事人 X 小姐在與一家與其有契約關係的電力公司之客服人員對話時，請求近用其資料。該人員對提出請求人的身分有疑問，因此透過公司系統產生一次性獨特代碼，作為雙重驗證系統之一環發送至使用者手機（其號碼係於辦理帳號時所提供）；此作法於本案中被視為符合比例原則。

67. In this context, it may be recalled that in situations in which the purposes for which the personal data are processed do not or no longer require the identification of a data subject the controller does not need to maintain identification data for the sole purpose of complying with data subjects' rights, also in light of the principle of

[26] Ibid, p. 14.
同前註，第 14 頁。
[27] Ibid, p. 13-14.
同前註，第 13-14 頁。

data minimisation. These situations are dealt with in Art. 11(1) GDPR.
於此情況下應注意，於運用個人資料之目的毋須或不再需要識別當事人的情況下，控管者毋須僅為遵循當事人權利而保留識別資料，此亦符合資料最小化原則。此等情況於 GDPR 第 11 條第 1 項中規範。

Example: A controller C processes personal data with the purpose of addressing behavioral advertising to its web users. Personal data collected for behavioral advertising are usually collected by cookies and associated with pseudonymous random identifiers. A data subject Mr. X exercises his right of access with C via C's website. C is able to precisely identify Mr. X to show the data subject's behavioral advertising, by linking the terminal equipment of Mr. X to its advertising profile with the cookies dropped in the terminal. C should then also be able to precisely identify Mr. X to grant him access to his personal data, as a link between the data processed and the data subject can be found.
範例：控管者 C 運用個人資料之目的為向其網路使用者提供行為定向廣告。為行為定向廣告所蒐集的個人資料通常係透過 cookies 蒐集，並與假名隨機識別碼相關。當事人 X 先生透過 C 的網站向 C 請求行使近用權。C 為投放行為定向廣告，透過其存放於 X 先生終端設備內的 cookies，將 X 先生的終端設備與其廣告檔案進行連結，據此精確識別 X 先生。因此 C 亦應能夠為向其提供個人資料之近用而精確識別 X 先生，因為其得識別被運用資料與當事人間之連結。

Therefore, and taking into account the principles of the GDPR, such as the principle of fairness, the above example would not fall within the scope of Art. 11 GDPR. More precisely, in the above example, the purposes of C require the identification of the data subjects, while Art. 11 GDPR addresses the situation of a controller who would process additional data within the meaning of Art. 11(1) GDPR for the sole purpose of being able to comply with the GDPR. Accordingly, Art. 11 should be interpreted in particular in the light of the principle of fairness. This, in some cases, may mean that no additional data should be requested in order to exercise the rights of the data subject.
因此，考量 GDPR 原則（如公平原則等），上述範例並不屬於 GDPR 第 11 條所規定範圍。更確切而言，於上述範例中，C 的運用目的需要識別當事人，而 GDPR 第 11 條是針對控管者專為遵守 GDPR 而運用 GDPR 第 11 條第 1 項所定額外資料的情況所設。因此，第 11 條應特別依據公平原則來解釋。於特定情況下，這可能表示不應為當事人權利之行使而要求提供額外資料。

However, if Mr. X tries to exercise his access right by e-mail or by regular mail,

then in this context C will have no other choice to ask Mr. X to provide "additional information" (Art. 12(6)) in order to be able to identify the advertising profile associated with Mr. X. In this case, the additional information will be the cookie identifier stored in the terminal equipment of Mr. X.
然而，若 X 先生試圖透過電子郵件或實體郵件行使近用權，則於此情況下，C 將不得不要求 X 先生提供「額外資訊」（第 12 條第 6 項），俾以識別與 X 先生相關之廣告檔案；於此情況下，額外資訊為儲存於 X 先生終端設備中的 cookie 識別碼。

68. In case of demonstrated impossibility to identify the data subject, the controller needs to inform the data subject accordingly, if possible, since the controller should generally be obliged to respond to requests from the data subject without undue delay and to give reasons where it does not intend to comply with such requests (Recital 59). This information needs to be provided only "if possible", as the controller may not be in a position to inform the data subjects if their identification is impossible.
若證明無法識別當事人，控管者需盡可能通知當事人，因控管者一般有義務對當事人之請求作出回覆，不得無故遲延，且應於拒絕遵守該等請求時提供理由（前言第 59 段）。此等資訊僅需於「有可能的情況下」提供，因為若無法識別當事人，控管者可能無法通知當事人。

3.3 Proportionality assessment regarding identification of the requesting person
關於識別請求人之比例性評估

69. As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable identification of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.
如上所述，若控管者有合理事由懷疑請求人的身分，得要求提供額外資訊以確認當事人身分。然而，控管者必須同時確保其所蒐集的個人資料不會超出識別請求人身分所必須之範圍。因此，控管者應進行比例性評估，必

須考量正在運用之個人資料類型（例如，是否為特種個人資料）、請求之性質、提出請求之背景，及任何可能因不當揭露而造成之損害。於評估比例性時，應確保避免過度蒐集資料，同時維持適當的運用安全水準。

70. The controller should implement an authentication (verification of the data subject's identity) procedure in order to be certain of the identity of the persons requesting access to their data[28], and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller imposes measures aimed at identifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).
控管者應進行認證（查驗當事人之身分）程序，以確認請求近用其資料者的身分[28]，並依據第 32 條規定，於處理近用請求之整個過程中確保運用之安全性，包括例如為當事人備置提供額外資訊的安全管道。認證方式應具相關性、適當性、符合比例原則及資料最小化原則。若控管者所採取識別當事人的措施相當繁瑣，則需為其提供適當事由，並確保遵守所有基本原則，包括資料最小化原則及促進當事人行使權利之義務（GDPR 第 12 條第 2 項）。

71. In accordance with Recital 57, identification should include the digital identification of a data subject. For example through authentication mechanism such as the same credentials, used by the data subject to log-in to the online service offered by the controller[29].
依據前言第 57 段，識別應包括當事人身分之數位識別。例如透過認證機制識別當事人登入控管者所提供線上服務所使用的憑證[29]。

72. In practice, authentication procedures often exist and controllers do not need to introduce additional safeguards to prevent unauthorised access to services. In order to enable individuals to access the data contained in their accounts (such as an e-

[28] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 14 頁。

[29] See further guidance regarding authentication methods in the EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 January 2021, p. 30-31., and in the EDPB Guidelines 02/2021 on virtual voice assistants , Version 2.0, Adopted on 7 July 2021, section 3.7.
關於認證方法之進一步指導，請參考 EDPB 個人資料侵害事件通報範例指引 01/2021（2021 年 1 月 14 日通過），第 30-31 頁，及 EDPB 虛擬語音助手指引 02/2021，第 2.0 版（2021 年 7 月 7 日通過），第 3.7 節。

mail account, an account on social networks or online shops), controllers are most likely to request the logging through the login and password of the user to authenticate, which in such cases should be sufficient to identify a data subject[30]. Consequently, it is disproportionate to require a copy of an identity document in the event where the data subject making their requests are already authenticated by the controller.

在實務上，控管者一般均已備有認證程序，而毋須導入額外保護措施來防止未經授權之近用。為使當事人能夠近用其帳戶中的資料（如電子郵件帳戶、社群網路上之帳戶或線上商店），控管者最有可能要求使用者輸入登入帳號及密碼來進行認證，於此情況下，這應足以識別當事人[30]。因此，若提出請求的當事人已通過控管者之認證，則要求當事人提供身分證明文件複製本並不符合比例原則。

73. It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

應強調者為，要求提供身分證明文件複製本作為認證流程的一部分，會使個人資料安全面臨風險，並可能導致未經授權或非法之運用，因此應被認為屬不適當，除非其屬絕對必要、適當，並符合國家法規。於此情況下，控管者應實施相應系統來確保安全水準，以緩解當事人為取得該等資料而使其權利及自由所面臨的較高風險。亦須注意者為，若當事人無法提供任何其他證據，例如符合使用者帳號之其他特徵資料，則透過身分證明文件進行身分識別，於線上的情境下並不一定有幫助（例如，因使用假名）。

74. Taking into account the fact, that many organisations (e.g. hotels, banks, car rentals) request copies of their clients' ID card, it should generally not be considered an appropriate way of authentication. Alternatively, the controller may implement a quick and effective security measure to identify a data subject who has been previously authenticated by the controller, e.g. via e-mail or text message

[30] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 14 頁。

containing confirmation links, security questions or confirmation codes[31].
考量到許多組織（如酒店、銀行、租車公司）會要求客戶提供身分證明文件複製本，一般而言，這不應被認為是一種適當的認證方式。或者，控管者得實施快速、有效的安全措施來識別其先前已完成認證的當事人，例如透過包含確認連結、安全問題或確認碼的電子郵件或簡訊[31]。

75. In any case, information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo and machine-readable zone, may be blackened or hidden by the data subject before submitting it to the controller, except where national legislation requires a full unredacted copy of the identity card (see para. 77 below). Generally, the date of issue or expiry date, the issuing authority and the full name matching with the online account are sufficient for the controller to verify the identity, always provided that the authenticity of the copy and the relation to the applicant are ensured. Additional information such as the birth date of the data subject may only be required in case the risk of mistaken identity persists, if the controller is able to compare it with the information it already processes.
無論如何，當事人得於將身分證明文件提交予控管者之前，將無涉身分確認的資訊（如近用號碼及序號、國籍、尺寸、眼睛顏色、照片及機器可讀碼）進行遮蔽或屏蔽，除非國家法規要求提供完整、未經遮蔽之身分證明文件複製本（見下文第 77 段）。一般而言，簽發日期或到期日期、簽發機關及符合線上帳戶的全名，即足以供控管者確認身分，但必須確保複製本的真實性及其與申請人之間的關係。只有在錯誤識別風險持續存在的情況下，才會需要取得當事人的額外資訊（如出生日期），以供控管者將其與已運用之資訊進行比較（如可能）。

76. To follow the principle of data minimisation the controller should inform the data subject about the information that is not needed and about the possibility to blacken or hide those parts of the ID document. In such a case, if the data subject does not know how or is not able to blacken such information, it is good practice for the controller to blacken it upon receipt of the document, if this is possible for the controller, taking into account the means available to the controller in the given circumstances.
為遵守資料最小化原則，控管者應告知當事人哪些資料毋須提供，及身分

[31] See also 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 and repealing Directive 1999/93/EC that has put forth different services that allow secure remote identification. 另見歐洲議會及歐盟理事會 2014 年 7 月 23 日關於內部市場電子交易之電子識別及信託服務之第 910/2014 號規則（歐盟），該規則廢除第 1999/93/EC 號指令（該指令提出可採用安全遠距識別的不同服務）。

證明文件中可以遮蔽或屏蔽的部分。於此情況下，若當事人不知道如何或無法將該等資訊遮蔽，則考量控管者於該等情況下可採用的方式，良好的作法為控管者應於收到文件後進行遮蔽（如可能）。

Example: The user Ms. Y has created an account in the online store, providing her e-mail and username. Subsequently, the account owner asks the controller for information whether it processes their personal data, and if so, asks for access to them within the scope indicated in Art. 15. The controller requests the ID of the person making request to confirm her identity. The controller's action in this case is disproportionate and leads to unnecessary data collection.
範例：使用者 Y 小姐於線上商店創建帳戶，提供其電子郵件及使用者名稱。隨後，帳戶所有人向控管者查詢是否有運用其個人資料，若有，則請求近用第 15 條所定範圍內資訊。控管者要求請求人提供身分證明文件以確認其身分。控管者之上述行為並不符合比例原則，屬不必要之資料蒐集。

However, the controller in order to confirm the identity of the requesting person, while preventing unnecessary data collection, could ask her (non-intrusive) security questions that were configured when the data subject registered their account, or it could employ multifactor authentication for access requests.
然而，控管者為確認請求人之身分，同時防止不必要之資料蒐集，得向其詢問（非侵入性的）安全問題（該等問題係由當事人註冊帳戶時所設定），或可針對近用請求實施多因素認證。

Example: A bank customer, Mr. Y, plans to get a consumer credit. For this purpose, Mr. Y goes to a bank branch to obtain information, including his personal data, necessary for the assessment of his creditworthiness. To verify the data subject's identity, the consultant asks for notarised certification of his identity to be able to provide him with the required information.
範例：銀行客戶 Y 先生計畫取得消費者信用貸款。為此目的，Y 先生到銀行分行取得評估其信用度所必須的相關資訊，包括其個人資料。為查驗當事人身分，銀行專員要求就其身分辦理公證認證，始得向其提供必要資訊。

The controller should not require notarised confirmation of identity, unless it is strictly necessary, suitable and in line with the national law (for example, where

a person is temporarily not in possession of any identity document and proof of the data subject's identity is required by the national law for the performance of a legal act). Such practice exposes the requesting persons to additional costs and imposes an excessive burden on the data subjects, hampering the exercise of their right of access.
控管者不應要求就其身分辦理公證認證，除非屬絕對必要、適當，且符合國家法規（例如，當事人暫時沒有任何身分證明文件，而國家法律規定在執行法律行為時必須提出當事人之身分證明）。此等做法使請求人面臨額外費用，並對當事人附加過度負擔，妨礙其近用權之行使。

77. Without prejudice to the above general principles, under certain circumstances, verification on the basis of an ID may be a justified and proportionate measure, for example for entities processing special categories of personal data or undertaking data processing which may pose a risk for data subject (e.g. medical or health information). However, at the same time, it should be borne in mind that certain national provisions provide for restrictions on the processing of data contained in public documents, including documents confirming the identity of a person (also on the basis of Art. 87 GDPR). Restrictions on the processing of data from these documents may relate in particular to the scanning or photocopying of ID cards or processing of official personal identification numbers[32].
以不影響上述一般原則為前提，於特定情況下，透過身分證明文件進行查驗可能屬合理且符合比例原則的措施，例如，對於運用特種個人資料或進行可能對當事人構成風險之資料運用的實體而言（例如，醫療或健康資訊）。然而，與此同時應注意者為，特定國家法規限制公共文書中資料之運用，包括確認個人身分之文件（GDPR 第 87 條亦有規定）。該等文件中資料之運用限制可能特別涉及掃描或複印身分證明文件或運用官方個人身分號碼[32]。

78. Taking the above into account, where an ID is requested (and this is both in line with national law and justified and proportionate under the GDPR), the controller must implement safeguards to prevent unlawful processing of the ID. Notwithstanding any applicable national provisions regarding ID verification, this may include not making a copy or deletion of a copy of an ID immediately after the successful verification of the identity of the data subject. This is because further storage of a copy of an ID is likely to amount to an infringement, in light of the

[32] Several member states introduced such restriction in their national provisions in this regard stating, for example, that making copies of ID cards is lawful only if it results directly from the provisions of a legal act. 若干會員國已在相關國家法規中引入該等限制，例如，製作身分證明文件之複製本，僅有在其係直接因執行合法行為所造成者始屬合法。

principles of purpose limitation and storage limitation (Art. 5(1)(b) and (e) GDPR) and any possible national legislation with regards to processing of the national identification number (Art. 87). The EDPB recommends, as good practice, that the controller, after checking the ID card, makes a note e.g. "ID card was checked" to avoid unnecessary copying or storage of copies of ID cards.
考量到上述情況，若要求提供身分證明文件（且符合國家法律，並於 GDPR 下屬合理且符合比例原則），控管者必須實施保護措施，防止非法運用身分證明文件。縱令有任何關於驗證身分證明文件之適用國家法規，這可能包括在成功驗證當事人身分後，不立即製作身分證明文件之複製本或刪除其複製本。這是因為依據目的限制原則及儲存限制原則（GDPR 第 5 條第 1 項第 b 及 e 款）及任何關於運用國家身分證字號之國家法規（第 87 條），進一步儲存身分證明文件複製本可能構成侵權。EDPB 建議，良好的作法為，控管者應於確認身分證明文件後進行相關註記，例如「已查驗身分證明文件」，以避免不必要地複製或儲存身分證明文件之複製本。

3.4 Requests made via third parties / proxies
透過第三人/代理人提出之請求

79. Although the right of access is generally exercised by the data subjects as it pertains to them, it is possible for a third party to make a request on behalf of the data subject. This may apply to, among others, acting through a proxy or legal guardians on behalf of minors, as well as acting through other entities via online portals. In some circumstances, the identity of the person authorised to exercise the right of access as well as authorisation to act on behalf of the data subject may require verification, where it is suitable and proportionate (see section 3.3 above). It should be recalled that making personal data available to someone who is not entitled to access it can amount to a personal data breach[33].
雖然近用權一般由當事人行使（因近用權與當事人有切身相關），但第三人有可能代表當事人提出請求。這可能適用（包括但不限於）代理人或法定監護人代表未成年人行事，及由其他實體透過線上入口網站行事的情況。於特定情況下，被授權行使近用權之人的身分及代表當事人行事之授權可能需要進行查驗（若屬適當且符合比例原則）（見上文第 3.3 節）。應注意者為，將個人資料提供予無權近用之人，會構成個人資料侵害事件[33]。

80. In doing so, national laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorization to make a request on behalf of the data subject, should be taken into account, since the

[33] Art. 4(12) GDPR.
GDPR 第 4 條第 12 項。

GDPR does not regulate this issue. In accordance with the principle of accountability, as well as of the other data protection principles, the controllers shall be able to demonstrate the existence of the relevant authorization to make a request on behalf of the data subject, except if national law foresees differently (e.g. specific rules regarding the trustworthiness of lawyers) leaving the controller the only obligation to verify the identity of the proxy (e.g. in the case of lawyers checking enrolment at the bar). Therefore, it is recommended to collect appropriate documentation in this respect, in relation to the previously indicated general rules regarding confirmation of identity of a natural person making a request and if the controller has reasonable doubts concerning the identity of a person acting on behalf of data subject, it shall request additional information to confirm the identity of this person.

這麼做應考量規範法律代表（如授權書）的國家法規，該等法規可能會對證明代表當事人提出請求之授權設有具體規範，因為 GDPR 並未對此議題作出規定。依據課責性原則及其他資料保護原則，控管者應證明存在可代表當事人提出請求相關授權，除非國家法規有不同規範（例如，關於律師可信度之具體規定），使控管者僅有義務查驗代理人的身分（例如，就律師而言，查驗其執業登記資格）。因此，建議在這方面蒐集適當文件，關於前述確認提出請求之自然人身分的一般規定，若控管者對當事人代表的身分有合理懷疑，即應要求提供額外資訊以確認其身分。

81. While the exercise of the right of access to personal data of deceased persons amounts to another example of access by a third party other than the data subject, Recital 27 specifies that the GDPR does not apply to the personal data of deceased persons. The matter is therefore dealt with by national law as Member States may provide for rules regarding the processing of personal data of deceased persons. However, it should be borne in mind that the data may in addition relate to living third persons, e.g. when it comes to the deceased's correspondence. The confidentiality of such data still needs to be protected.

而對已故人士之個人資料行使近用權，則是由當事人以外之第三者近用之另一例子；前言第 27 段說明，GDPR 不適用已故人士之個人資料。因此，此議題由國家法律處理，因為會員國得訂定關於運用已故人士個人資料之規定。然而，應注意者為，該等資料可能亦涉及生存之第三人，例如涉及已故人士之通訊。該等資料之機密性仍然需要保護。

3.4.1 Exercise of the right of access on behalf of children
代表兒童行使近用權

82. Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerning their rights in

relation to the processing of personal data[34]. Any information and communication to a child, where personal data of a child are processed, should be in such a clear and plain language that the child can easily understand[35].
兒童於其個人資料方面應得到特別保護，因為兒童可能不太瞭解關於個人資料運用之風險、後果及權利保障[34]。於運用兒童之個人資料時，對兒童提供之任何資訊及溝通均應以兒童能夠輕易理解的清晰、簡明語言進行[35]。

83. Children are data subjects in their own right and, as such, the right of access belongs to the child. Depending on the maturity and capacity of the child, acting on behalf of the child by the holder of the parental responsibility could be needed.
兒童就其本身權利而言亦屬當事人，因此兒童亦擁有近用權。取決於個別兒童的成熟度及能力，可能需要由親權人代表兒童行事。

84. The best interests of the child should be the leading consideration in all decisions taken with respect to the exercise of the right of access in the context of children, in particular where the right of access is exercised on behalf of the child, for example by the holder of parental authority.
於針對兒童行使近用權作出任何決定時，應以兒童的最大利益為首要考量，特別是在他人（例如親權人）代表兒童行使近用權的情況。

85. Due to the special protection of children's personal data contained in the GDPR, the controller shall take appropriate measures to avoid any disclosure of personal data of a minor to an unauthorised person (in this respect see also section 3.4 above).
因 GDPR 中對兒童個人資料之特別保護，控管者應採取適當措施，避免向未經授權之人揭露未成年人之個人資料（於此方面另見上文第 3.4 節）。

86. Finally, the right of the holder of parental responsibility to act on behalf of the child should not be confused with instances, outside of data protection law, where the national legislation may provide the right of the holder of parental responsibility to ask and receive information on the child (e.g. performance of the child at school).
最後，親權人代表兒童行事之權利不應與資料保護法律以外之情況混為一談，於該等情況下，國家法規可能允許親權人詢問及取得關於兒童之資訊

[34] Recital 38 GDPR. As provided in the working programme of EDPB, it is its intent to provide guidance on children's data. Such a document is expected to provide more guidance on the conditions under which a child may exercise their own right of access, and the holder of parental responsibility can exercise the right of access on behalf of the child.
GDPR 前言第 38 段。如 EDPB 之工作計畫所載，其目的為提供關於兒童資料之指導。該等文件預計將提供更多關於兒童得行使自身近用權及親權人得代表兒童行使近用權之條件的指導。

[35] Recital 58 GDPR. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, section 7.
GDPR 前言第 58 段。EDPB 關於第 2016/679 號規則下同意之指引 05/2020，第 7 節。

（例如，兒童在校表現）。

3.4.2 Exercising the right of access through portals / channels provided by a third party
透過第三人提供之入口網站/管道行使近用權

87. There are companies that provide services which enable data subjects to make access requests through a portal. The data subject signs in and gets access to a portal through which they can submit for example an access request, request data rectification or data erasure from different controllers. Different questions arise from the use of portals provided for by a third party.
有些公司提供可使當事人透過入口網站提出近用權請求之服務。當事人登入並連接至入口網站後，可透過該網頁提交如近用權、更正或刪除自不同控管者的資料等請求。於使用由第三人提供的入口網站時，會出現不同的問題。

88. The first issue controllers need to deal with when facing these circumstances refers to ensuring that the third party is acting legitimately on behalf of the data subject, as it is necessary to make sure that no data is disclosed to unauthorised parties.
於面對該等情況時，控管者需要處理的第一個問題，是確保第三人係合法代表當事人行事，因其有必要確保不將資料揭露予未經授權之人。

89. Additionally, a controller that receives a request made through such a portal needs, invariably, to handle that request in a timely manner. There is, however, no obligation for the controller to provide the data under Art. 15 directly to the portal. If the controller, for example, establishes that the security measures are insufficient, it would be deemed appropriate to use another way for the disclosure of data to the data subject. Under such circumstances, when the controller has other procedures in place to deal with access requests in an efficient way, the controller can provide the requested information through these procedures.
此外，控管者在收到透過該等入口網站提出之請求時，同樣需要迅即處理該等請求。然而，控管者無義務直接向該等入口網站提供第 15 條所定資料。例如，若控管者認定安全措施不足，則採用其他方式向當事人揭露資料將被認為屬適當作法。於此情況下，當控管者備有其他程序得有效處理近用請求時，控管者得透過該等程序提供所請求之資訊。

4 SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS
近用權之範圍及其涉及之個人資料及資訊

90. The present section aims at shedding light on the definition of personal data (4.1)

and clarifying the scope of the information covered by the right of access in general (4.2 and 4.3). Of note is that the scope of the notion of personal data and thus, the differentiation between personal data and other data, is an integral part of the assessment carried out by the controller to identify the scope of the data that the data subject is entitled to obtain access to[36].
本節旨在說明個人資料之定義（第 4.1 節）及釐清近用權一般涵蓋的資訊範圍（第 4.2 及 4.3 節）。值得注意者為，個人資料概念之範圍，及個人資料及其他資料間之區別，是控管者於針對當事人有權近用資料之範圍所進行評估之重要組成部分[36]。

91. As a preliminary consideration it should be recalled that the right of access can only be exercised with regard to processing of personal data falling within the material and territorial scope of the GDPR. Therefore, personal data that are not processed by automated means or that are not part of or intended to become part of a filing system as per Art. 2(1) GDPR, or processed by a natural person in the course of a purely personal activity as per Art. 2 (2) GDPR, are not covered by the right of access.
於進行初步考量應注意，近用權之行使僅得針對屬 GDPR 之客體及地域適用範圍內的個人資料運用。因此，並非透過自動化方式運用之個人資料、並非於 GDPR 第 2 條第 1 項下屬於或將成為歸檔系統一部分之個人資料，或依據 GDPR 第 2 條第 2 項由自然人於單純個人活動中運用之資料，均不屬於近用權範圍。

4.1 Definition of personal data
個人資料之定義

92. Art. 15(1) and (3) GDPR refer to "*personal data*", and "*personal data undergoing processing*", respectively. Therefore, the scope of the right of access is first and foremost determined by the scope of the concept of personal data, defined in Art. 4(1) GDPR[37]. The concept of personal data has already been the subject of several

[36] In accordance with the principle of privacy by design, such analysis is part of the assessment of appropriate measures and safeguards to protect data protection principles and data subject rights, which is carried out "*at the time of the determination of the means for processing and at the time of the processing itself*", e.g. reducing the response time when data subjects exercise their rights may be one of the metrics. For further explanations, see guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
依據隱私權設計保護原則，該等分析係關於維護資料保護原則及當事人權利之適當措施及保障措施評估的一部分，該等評估係於「*判斷運用方式時及運用本身時*」進行，例如，縮短當事人行使其權利時之回覆時間可能是衡量標準之一。進一步說明請見關於第 25 條資料保護之設計及預設指引 4/2019。

[37] As per Art. 4 (1) GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Art. 29 Working Party[38] documents[39] and has been interpreted by the CJEU, including in the context of the right of access under Art. 12 of the Directive 95/46/CE.

GDPR 第 15 條第 1 項及第 3 項分別提及「*個人資料*」及「*正在被運用之個人資料*」。因此，近用權之範圍首先且多數係由 GDPR 第 4 條第 1 項所定義之個人資料概念的範圍決定[37]。個人資料之概念已成為多份第 29 條工作小組[38]文件的主題[39]，並由歐盟法院作出解釋，包括第 95/46/CE 號指令第 12 條下之近用權脈絡。

93. The WP29 considered that the definition of personal data in the Directive 95/46/EC "*reflects the intention of the European lawmaker for a wide notion of 'personal data'*"[40]. Under the GDPR, the definition still refers to "*any information relating to an identified or identifiable natural person*". Aside from basic personal data like name and address, telephone number etc., unlimited broad variety of data may fall within this definition, including medical findings, history of purchases, creditworthiness indicators, communication contents, etc. In light of the broad scope of the definition of personal data, a restrictive assessment of that definition by the controller would lead to an erroneous classification of personal data[41] and ultimately to a violation of the right of access.

第 29 條工作小組認為，第 95/46/EC 號指令中之個人資料定義「*反映歐洲立法者賦予個人資料廣泛概念之意圖*」[40]。依據 GDPR，該定義仍然係指「*與已識別或可識別身分之自然人相關的任何資訊*」。除基本個人資料（如姓名、地址、電話號碼等）外，其他廣泛類型之資料均可能屬此定義範圍，如醫療結果、購買紀錄、信用指標、通訊內容等。有鑑於個人資料定義之廣泛範圍，控管者若對此定義進行限制性評估，將會導致個人資料之錯誤

GDPR 第 4 條第 1 項：「個人資料係指與已識別或可識別身分之自然人（當事人）相關的任何資訊。可識別身分之自然人係指得直接或間接識別其身分之人，特別是透過參考諸如姓名、識別碼、位置資料、線上識別碼等識別碼或與該自然人之身體、生理、基因、心理、經濟、文化或社會身分相關的一項或多向因素；」

[38] The Art. 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR), the predecessor of the EDPB.
第 29 條工作小組為獨立的歐洲工作小組，負責處理與隱私權及個人資料保護相關的議題，直到 2018 年 5 月 25 日為止（GDPR 生效之日），為 EDPB 之前身。

[39] e.g. WP251 rev01 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 i.e., p.19; WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9.
例如，WP251 修訂一版，關於 2016/679 號規則下自動化個別決策及剖析之指引，第 19 頁；第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 9 頁。

[40] WP29 Opinion 4/2007 on the concept of personal data, p. 4.
第 29 條工作小組關於個人資料概念之第 4/2007 號意見，第 4 頁。

[41] as information not relating to an identified or identifiable natural person
作為不涉及已識別或可識別身分之自然人的資訊

分類，[41]，並最終造成違反近用權。

94. In joint cases C-141/12 and C-372/12[42] the CJEU ruled that the right of access covered personal data contained in minutes, namely the "*name, date of birth, nationality, gender, ethnicity, religion and language of the applicant*" "*and, "where relevant, the data in the legal analysis contained in the minute*", but not the legal analysis itself[43]. The legal analysis was in this context not liable in itself to be the subject of a check of its accuracy by the data subject nor of a rectification. Furthermore, providing access to the legal analysis does not fulfil the purpose of guaranteeing privacy but access to administrative documents.
於 C-141/12 及 C-372/12 合併案件中 [42]，歐盟法院認定，近用權包括會議紀錄中之個人資料，即「*申請人之姓名、出生日期、國籍、性別、種族、宗教及語言*」及「*於相關情況下，會議紀錄中之法律分析資料*」，但不包括法律分析本身 [43]。於此情況下，法律分析本身並非當事人檢查其正確性或更正之標的。此外，對法律分析提供近用並不能達到保障隱私權之目的，而是行政文件之近用。

95. In Nowak[44], the CJEU made a broader analysis and found that written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers constitute personal data concerning the exam candidate. More precisely, such subjective information are personal data "*in the form of opinions and* assessments, *provided that it 'relates' to the data subject*"[45] as opposed to the examination questions, which are not considered personal data[46]. Thus, a contextual assessment should shed light on the effect or result an information may have on an individual and thus the scope of the right of access.
於 Nowak 一案中 [44]，歐盟法院進行更廣泛的分析，認定考生於專業考試中提交的書面答案及考官對該等答案之任何評論均構成該考生之個人資料。更確切而言，該等主觀資訊屬「*意見及評價形式*」之個人資料，但前提為

---

[42] Court of Justice of the European Union, Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, 17 July 2014.
歐盟法院，合併案件 C-141/12 及 C-372/12，YS 訴 Minister voor Immigratie 與 Integratie en Asiel；及 Minister voor Immigratie 與 Integratie en Asiel 訴 M 及 S，2014 年 7 月 17 日。

[43] CJEU, Joined Cases C-141/12 and C-372/12, YS and Others, paras. 38 and 48.
歐盟法院，合併案件 C-141/12 及 C-372/12，YS 及他人，第 38 及 48 段。

[44] Court of Justice of the European Union, C-434/16, Peter Nowak v Data Protection Commissioner, 20 December 2017.
歐盟法院，C-434/16 案，Peter Nowak 訴資料保護委員會，2017 年 12 月 20 日。

[45] CJEU, C 434/16, Nowak, paras. 34- 35.
歐盟法院，C434/16（Nowak 案），第 34-35 段。

[46] CJEU, C-434/16, Nowak, para. 58.
歐盟法院，C-434/16（Nowak 案），第 58 段。

「*其與當事人相關*」[45]，而與考試題目不同，其不被視為個人資料[46]。因此，情境評估應檢視資訊對個人可能產生的影響或後果，從而判斷近用權的範圍。

Example: An individual has a job interview with a company. In this context, the job applicant hands over a CV and an application letter. During the interview, the HR officer takes notes on a computer to document the interview. Afterwards, the job applicant, as data subject requests access to personal data relating to them that the company, as controller, collected in the course of the recruitment procedure.
範例：當事人與一家公司進行一次工作面試。於此情況下，該求職者提交了一份簡歷及一封申請書。於面試過程中，人資主管於電腦上紀錄面試過程。之後，求職者以當事人身分請求近用該公司作為控管者於招聘過程中蒐集與其相關之個人資料。

The controller is obliged to provide the data subject with personal data actively communicated by them in their CV and letter of application. Moreover, the controller needs to provide the data subject with the summary of the interview, including the subjective comments on the behaviour of the data subject the HR officer wrote during the job interview.
控管者有義務向當事人提供其於簡歷及申請書中主動提供的個人資料。此外，控管者需要向當事人提供面試摘要，包括人資主管於工作面試中對當事人行為所作之主觀評價。

96. Thus, subject to the specific facts of the case, when assessing a specific request for access, the following types of data are, *inter alia*, to be provided by controllers without prejudice to Art. 15(4) GDPR:
因此，依據案件之具體事實，於評估具體近用請求時，以不影響 GDPR 第 15 條第 4 項為前提，控管者應提供以下類型之資料：

- Special categories of personal data as per Art. 9 GDPR;
  GDPR 第 9 條所定特種個人資料；

- Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
  GDPR 第 10 條所定與前科及犯罪相關之個人資料；

- Data knowingly and actively provided by the data subject (e.g. account

data submitted via forms, answers to a questionnaire)[47];
當事人知情、主動提供的資料（如透過表單提交之帳戶資料，於問卷中提供的回覆）[47]。

- Observed data or raw data provided by the data subject by virtue of the use of the service or the device (data processed by connected objects, transaction history, activity logs such as access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking or speaking) [48];
當事人因使用服務或設備而提供之觀察資料或原始資料（由連接物件運用之資料、交易紀錄、活動日誌，如近用日誌、網站使用紀錄、搜尋活動、位置資料、點擊活動、個人行為之獨特面向，如筆跡、擊鍵、特殊的行走或說話方式等）[48]；

- Data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects; country of residence derived from postcode)[49];
自其他資料推論出之資料，而非由當事人直接提供之資料（例如信用比率，以當事人共同屬性為基礎之分類；自郵遞區號推論出之居住國）[49]；

- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)[50];
自其他資料推論出之資料，而非由當事人直接提供之資料（例如，打出信用分數或遵守洗錢防制規定、演算法結果、健康評估結果或個人化或推薦流程）[50]；

---

[47] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9.
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 9 頁。

[48] WP29 Opinion 4/2007 on the concept of personal data, p. 8
第 29 條工作小組關於個人資料概念之第 4/2007 號意見，第 8 頁。

[49] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10-11
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 10-11 頁。

[50] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p.10-11; Art. 29 Working Party, WP 251 rev.01, 6 February 2018, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB"), p. 9-10.
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可），第 10-11 頁；第 29 條工作小組 WP251 修訂一版，2018 年 2 月 6 日，關於 2016/679 號規則下自動化個別決策及剖析之指引－經 EDPB 認可（以下簡稱「第 29 條工作小組自動化個別決策及剖析指引（經 EDPB 認可）」），第 9-10 頁。

- Pseudonymised data as opposed to anonymized data (see also section 3 of these guidelines).
  假名化資料（而非匿名化資料）（另見本指引第 3 節）。

Example: Elements that have been used to reach a decision about e.g. employee's promotion, pay rise or new job assignment (e.g. annual performance reviews, training requests, disciplinary records, ranking, career potential) are personal data relating to that employee. Thus such elements can be accessed by the data subject on request and respecting Art.15 (4) GDPR in case personal data for example, also relate to another individual (e.g. the identity or elements revealing the identity of another employee whose testimony about the professional performance is included in an annual performance review may be subject to limitations under Art. 15(4) GDPR and hence it is possible that they cannot be communicated to the data subject in order to protect the rights and freedoms of said employee). Nevertheless, national labour law provisions may apply for instance regarding the access to personnel files by employees or other national provisions such as those concerning professional secrecy. Under all circumstances, such restrictions to the exercise of the right of access of the data subject (or other rights) provided in a national law must respect the conditions of Art. 23 GDPR (see section 6.4).
範例：用來決定員工晉升、加薪或新工作分配之元素（如年度績效評估、訓練要求、懲戒紀錄、排名、職涯潛力等）均屬該員工之個人資料。因此，即使在該等資料同時涉及他人的情況下（例如，年度績效評估中對當事人績效作出評論之其他員工身分，或會揭露其身分之元素，可能會受到 GDPR 第 15 條第 4 項之限制，因此有可能無法提供予當事人，以保護該等員工之權利及自由）。然而，國家勞動法律或其他關於專業保密義務的國家法規可能適用員工近用其人事檔案事宜。無論如何，國家法律對行使近用權（或其他權利）所設限制，必須符合 GDPR 第 23 條所定條件（見 6.4 節）。

97. Several considerations may be drawn from the above non-exhaustive list of personal data which may be provided to the data subject in case of an access request. It becomes for instance notably apparent from the above, that the controller may not operate a distinction when providing access between personal data contained in paper files and those stored electronically as long as they fall within the scope of the GDPR. In other words, personal data which are contained in paper files as part of a filing system, or which are intended to form part of a filing system, are covered by the right of access in the same way as personal data stored in a computer memory by means of binary code, or on a videotape.

自上述可依據近用請求提供予當事人之個人資料例示（非詳盡）清單中可推論出若干考量因素。例如，自上述內容可明顯看出，只要相關個人資料屬 GDPR 範圍，控管者於提供近用時不得區分儲存於紙本文件中的個人資料及以電子形式儲存的個人資料。換言之，作為歸檔系統（或將成為歸檔系統）之一部分而包含於紙本文件中的個人資料，與以二進位碼方式儲存在電腦記憶體中或儲存在錄影帶內的個人資料一樣，均屬於近用權之範圍。

98. Moreover, like most data subject rights, the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject[51]. Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment. 此外，與大部分當事人權利一樣，近用權包括推論及衍生資料，包括由服務供應商創建之個人資料，而資料可攜權僅包括由當事人提供的資料 [51]。因此，近用請求與資料可攜請求的不同點為，當事人不僅應取得其先前為進行後續分析或評估而提供予控管者之個人資料，且亦應取得任何該等後續分析或評估之結果。

99. It also is important to recall that there is information, such as anonymous data[52], which is data that do not relate directly or indirectly to an identifiable person, and that are hence excluded from the scope of the GDPR. For example, the location of the server on which the personal data of the data subject processed is not personal data. The distinction can be challenging and controllers may wonder how to draw a clear line between personal and non-personal data in particular in the case of mixed datasets. In such case it may be useful to differentiate between mixed datasets in which personal and nonpersonal data are inextricably linked and those in which this is not the case. Personal and non-personal data may be inextricably linked in mixed datasets and fall altogether under the scope of the right of access

[51] As previously stated in WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10 and reiterated in WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB, p. 17.
如先前於第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）中所述，第 10 頁；及於第 29 條工作小組自動化個別決策及剖析指引（經 EDPB 認可）中所重申，第 17 頁。

[52] Further explanations on the concept of anonymization can be found in Art. 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 April 2014, p. 5-19.
關於匿名化概念之進一步說明可參考第 29 條工作小組關於匿名化技術之第 05/2014 號意見（WP216），2014 年 4 月 10 日，第 5-19 頁。

of the data subject to which the personal data relates[53]. In other cases personal and nonpersonal data in mixed datasets may not be inextricably linked rendering only the personal data in the set accessible to the data subject. For example, a company might need to provide a data subject with the individual IT incident reports it triggered, but not with the company's knowledge database of IT problems. However, which security measures the controller has put in place is generally not to be understood as being personal data, provided that these are not inextricably linked with personal data, and therefore not covered by the right of access.
另應注意者為，有些資訊非屬 GDPR 之範圍，如匿名化資料 [52]，因為其不是直接或間接與可識別身分之人相關的資料。例如，運用當事人個人資料之伺服器位置即非屬個人資料。做此區分可能具有挑戰性，控管者可能會想瞭解如何在個人及非個人資料之間劃出一條明確的界限，特別是遇到混合資料集的情況下。於此情況下，將個人及非個人資料密不可分的混合資料集及其他混合資料集先進行區分會相當有用。於混合資料集中，個人及非個人資料可能是密不可分，並完全屬於當事人就其個人資料行使近用權的範圍 [53]。於其他情況下，混合資料集中的個人及非個人資料可能不存在密不可分的情況，因此僅有其中的個人資料需提供予當事人。例如，一家公司可能需要將個別資安事件通知當事人，但毋須向當事人提供其資安議題知識資料庫內容。然而，控管者所採取的安全措施一般不應被理解為個人資料（但前提為該等措施與個人資料不存在密不可分的情況），因此非屬近用權範圍。

100. Before concluding the section, the EDPB recalls in this context that the protection of natural persons with regard to the processing of personal data encompasses all the types of personal data listed above and that a restrictive interpretation of the definition contravenes the provisions of the GDPR and ultimately violates Art. 8 of the Charter of Fundamental Rights. The application of a differing regime for the exercise of a right in relation to some types of personal data, which has not been foreseen by the GDPR can be introduced exclusively by law, in accordance with Art. 23 GDPR (as further explained in section 6.4). Thus, controllers cannot limit the exercise of the right of access by unduly restricting the scope of personal data.
本節結束前，EDPB 重申，於運用個人資料方面，對自然人的保護涵蓋上述所有類型的個人資料，對此定義之限制性解釋違反 GDPR 規定，最終亦違反歐盟基本權利憲章之第 8 條。依據 GDPR 第 23 條，GDPR 未預見之需採行不同制度之特定類型之個人資料權利行使，僅能透過法律規範（於第 6.4

[53] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29.05.2019, COM/2019/250 final. 歐盟執委會致歐洲議會及歐盟理事會之信函，關於歐盟非個人資料自由流動框架規則之指導，2019 年 5 月 29 日，COM/2019/250（定稿版）。

節進一步說明）。因此，控管者不得透過不當限縮個人資料範圍來限制近用權之行使。

4.2 The personal data the right of access refers to
近用權所指之個人資料

101. According to Art. 15(1) GDPR, "*the data subject shall have the 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 and the following information*"(emphasis added).
GDPR 第 15 條第 1 項：「*當事人有權向控管者確認關於他/她的個人資料是否正在被運用，若是，則近用其個人資料及以下資訊*」（原文無底線標記）。

102. Several elements emerge from paragraph (1) of Art. 15 GDPR. The paragraph refers *expressis verbis* to "*personal data concerning him or her*"(4.2.1) , which "*are being processed*"(4.2.2) by the controller:
GDPR 第 15 條第 1 項有幾個要素，該項*明確*提及「*關於他/她的個人資料*」（第 4.2.1 節）及「*正在被控管者運用*」（第 4.2.2 節）。

4.2.1 "personal data concerning him or her"
「關於他/她的個人資料」

The right of access can be exercised exclusively with regard to personal data relating to the data subject requesting access or, where applicable, by an authorised person or proxy (see section 3.4). There are also situations in which data do not have a link to the person exercising the right of access but to another individual. The data subject is however, only entitled to personal data relating to themselves excluding data which exclusively concern someone else [54] .
近用權僅得針對與請求近用之當事人相關之個人資料行使，或於適用的情況下，由被授權人或代理人行使（見第 3.4 節）。另有一種情況是，資料與行使近用權之人沒有關聯，而是與其他個人有關聯。然而，當事人僅有權取得與自身相關之個人資料，不包括僅涉及他人之資料[54]。

103. The classification of data as personal data concerning the data subject does

[54] WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9: "*Only personal data is in scope of a data portability request. Therefore, any data that is anonymous 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 them providing the respective identifier, cf. Article 11 (2)) is within the scope.*"
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）第 9 頁：「*僅有個人資料屬於資料攜帶請求之範圍內。因此，任何匿名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。*」

however not depend upon the fact that those personal data also relate to someone else[55]. It is thus possible that personal data relate to more than one individual at the same time. This does not automatically mean that access to personal data also relating to someone else should be granted, as the controller needs to comply with Art. 15(4) GDPR.

然而，將資料歸類為當事人個人資料，並不取決於該等個人資料是否亦與他人相關[55]。因此，個人資料有可能同時與多人相關。這並不必然代表亦應允許對涉及他人之個人資料之近用，因控管者必須遵守 GDPR 第 15 條第 4 項規定。

104. The words "*personal data concerning him or her*" should not be interpreted in an "*overly restrictive*" way by controllers, as the Art. 29 Working Party already stated with regard to the right to data portability[56]. Transposed to the right of access, the EDPB considers for example that recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may fall under the right of access provided that the latter are personal data[57]. Provided that the GDPR applies and that the processing is not covered by the household exemption as per Art. 2(2)(c) GDPR, if the data subject uses the obtained record which includes personal data of the interlocutor for other purposes by, for instance, publishing the record, the data subject will become a controller for this processing of personal data relating to the other person whose voice was recorded. Although this will not exempt the controller from its data protection obligations when duly analysing whether access to the full record may be given, the controller should inform the data subject about the fact that they may become controller in such case.

---

55 EUCJ, judgment in case C-434/16 Peter Nowak v. Data Protection Commissioner, 2017, para. 44.
歐盟法院，就 C-434/16 案，Peter Nowak 訴資料保護委員會之判決，2017 年，第 44 段。

56 WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9:" *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).*"
第 29 條工作小組關於資料可攜權之指引（經 EDPB 認可）第 9 頁：「*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）。*」

57 See example 1 in section 6.2.
見第 6.2 節範例 1。

This is without prejudice to any further assessment under Art. 15(4) GDPR detailed in section 6. In the same vein, messages that data subjects have sent to others in the form of interpersonal messages and deleted themselves from their device, that are still available to the service provider, may fall under the right of access.

如同第 29 條工作小組曾就資料可攜權所述，控管者不應以「*過度限縮*」的方式解釋「*關於他/她的個人資料*」[56]。將其套用於近用權上，EDPB 認為，舉例而言，當事人請求近用與控管者間之通話錄音（及其逐字稿）可能屬於近用權範圍，但前提是後者屬個人資料[57]。只要適用 GDPR，且該運用不屬於 GDPR 第 2 條第 2 項第 c 款所定家庭豁免範圍，若當事人使用其中包括對話者個人資料之錄音作為其他目的（例如，發布該錄音），就運用錄音中通話對象之個人資料而言，當事人將成為控管者。雖然這不會免除控管者於適當分析是否得提供完整錄音之近用時之資料保護義務，但控管者應告知當事人，其於此情況下可能成為控管者。這並不影響第 6 節所述依據 GDPR 第 15 條第 4 項之任何進一步評估。同樣地，當事人以私人通訊之形式向他人發送並自行從其裝置上刪除的資訊，若服務供應商仍可取得，則可能屬近用權範圍。

105. Then again, there are situations in which the link between the data and several individuals may seem blurred to the controller, such as in the case of identity theft. In case of identity theft, a person fraudulently acts in the name of another person. In this context it is important to recall that the victim should be provided with information on all personal data the controller stored in connection with their identity, including those that have been collected on the basis of the fraudster's actions. In other words, even after the controller learned about the identity theft, personal data is associated with or related to the identity of the victim and therefore constitutes personal data of the data subject.

然而，在有些情況下，資料及多名個人間之連結就控管者看來可能不太明確，例如於身分冒用的情況下。在發生身分冒用時，冒用者以他人名義進行詐欺。於此情況下，應注意者為，應向受害人提供控管者所儲存與其身分相關之所有個人資料的資訊，包括基於詐欺者之行為而蒐集之資訊。換言之，即使於控管者知悉身分冒用後，個人資料仍與受害人之身分相關或連結，因此構成當事人之個人資料。

Example: An individual fraudulently uses the identity of someone else in order to play poker online. The perpetrator pays the online casino using the credit card they stole from the victim. When the victim finds out about the identity theft, the victim asks the provider of the online casino to provide him or her with access

to personal data relating to him or her and more specifically to the online games played and information about the credit card used by the perpetrator.
範例：犯罪人以詐欺方式使用他人身分玩線上撲克，使用自受害人處偷來的信用卡向線上賭場付款。當受害人發現身分遭冒用時，要求線上賭場營運商提供與其相關的個人資料，特別是提供與其所玩線上遊戲及犯罪人所使用的信用卡相關之資訊。

There is a link between the collected data and B as the latter's identity has been used. After the detection of the fraud, the personal data mentioned above still has a link by reason of their content (the victim's credit card is clearly about the victim), purpose and effect (the information about the online games played by the perpetrator may for instance be used to issue invoices to the victim). Therefore, the online casino shall grant the victim access to the aforementioned personal data.
所蒐集資料與 B 之間存在連結，因為後者的身分曾遭使用。於發現詐欺行為後，上述個人資料因其內容（受害人之信用卡顯然與受害人有關連）、目的及效果（例如，犯罪人所玩線上遊戲之資訊可能被用來向受害人開立發票）而仍然與受害人有所連結。因此，線上賭場應授予受害人近用上述個人資料。

106. The putting in place and the supervision and revision of connection logs[58] fall within the controller's responsibility and are liable to be checked by the supervisory authorities. The controller should thus make sure that the persons acting under its authority who have access to personal data do not process personal data except on instructions from the controller, as per Art. 29 GDPR. If the person nevertheless processes the personal data for other purposes than fulfilling the controller's instructions, it may become controller for that processing and subject to disciplinary or criminal proceedings or administrative sanctions issued by Supervisory Authorities. The EDPB notes that it is part of the employer's responsibility under Art. 24 GDPR to make use of appropriate measures, extending from education to disciplinary procedures, to ensure that processing is in compliance with the GDPR and that no data breach occurs.
備置、監管及修訂連線日誌 [58] 屬控管者之責任範圍，且應負責提供該等日誌供監管機關查驗。因此，依據 GDPR 第 29 條，控管者應確保，依其授權行事且有權近用個人資料之人，不會運用個人資料，除非係依據控管者之

[58] A request for a preliminary ruling from the Itä-Suomen hallinto-oikeus (Finland) lodged on 22 September 2021 — J.M. Case C-579/21 is pending before the CJEU at the time of the publication of the public consultation version of these guidelines.
2021 年 9 月 22 日 Itä-Suomen hallinto-oikeus（芬蘭）提出之初步裁決請求－J.M.案 C-579/21，於本指引之公眾諮詢版本發布時，正在等待歐盟法院之裁決。

指示。若該人為履行控管者指示以外之其他目的運用個人資料，則其可能成為該等運用之控管者，並因此受到懲戒或刑事訴訟或監管機關之行政處分。EDPB 指出，依據 GDPR 第 24 條，採取適當措施為雇主責任之一，包括實施教育訓練到懲戒程序，以確保運用符合 GDPR 及不會發生資料侵害事件。

4.2.2 Personal data which "are being processed"
「正在被運用」的個人資料

107. Paragraph (1) of Art. 15 GDPR moreover refers to personal data, which "are being processed". The time reference point for determining the range of personal data falling within the access request has already been elaborated in section 2.3.3. The wording however also suggests that the right of access does not distinguish between the purposes of the processing operations.
GDPR 第 15 條第 1 項進一步提及「正在被運用」的個人資料。用於確認是否屬近用請求範圍之個人資料的時間參考點已於第 2.3.3 節中說明。然而，此用語亦顯示，近用權並不以運用作業目的做為區分。

> **Example**: A company processed personal data relating to a data subject in order to process their purchase order and arrange shipping to data subject's home address. After these initial purposes for which the personal data were collected do no longer exist, the controller keeps some of the personal data solely to comply with its legal obligations relating to the keeping of records.
> **範例**：一家公司曾運用與當事人相關之個人資料，以處理其採購訂單，並安排出貨至當事人之住家地址。於該等最初蒐集個人資料之目的不復存在後，控管者僅為履行其保存紀錄之法律義務而保留特定個人資料。
>
> The data subject requests access to personal data relating to them. To comply with its obligation under article 15 (1) GDPR, the controller needs to provide the data subject with the requested personal data which are stored to comply with its legal obligations.
> 當事人請求近用與其相關之個人資料。為遵守 GDPR 第 15 條第 1 項所定義務，控管者需向當事人提供其為遵守法律義務而保存該當事人請求之個人資料。

108. Archived personal data needs to be distinguished from back-up data that is personal data stored solely for the purpose of restoring the data in the case of a data loss event. It should be pointed out, that in respect of the principles of data protection by design and data minimisation, the back-up data is in principle similar

to the data in the live system. Where there are slight differences between personal data in the back-up and the live production system, these are generally linked to the collection of additional data since the last back-up. A decrease in data in the live system (e.g. erasure after the retention period of some data came to an end or following an erasure request) will in some cases only be overwritten in the back-up data at the time of the subsequent back-up. In case there is an access request at the moment where there are more personal data relating to the data subject in the backup than in the live system or different personal data (noticeable for example via log of deletions in the live production system implemented in full compliance with the principle of data minimisation), the controller needs to be transparent about this situation and where technically feasible provide access as requested by the data subject, including to personal data stored in the back-up. For instance, with the aim of being transparent to the data subject that exercises their right, a log of deletions in the live production system may enable the controller to see that there are data in the back-up which are no more in the live system as they have been deleted shortly, which has not yet been overwritten in the back-up.
歸檔之個人資料需與備份資料有所區隔，後者係僅為於資料滅失事件中回復資料而保存的個人資料。應注意者為，就資料保護設計及資料最小化原則而言，備份資料原則上與即時系統中的資料相似。若備份之個人資料及即時生產系統中之個人資料有細微差異，該等差異通常係關於自上次備份後所蒐集的額外資料。即時系統中之資料減少時（例如，於特定資料之保存期間終了後或依請求而刪除），於特定情況下僅會於後續備份時於備份資料中遭覆蓋。在當事人提出近用請求時，若備份中與該當事人相關之個人資料比在即時系統中多，或存在不同的個人資料（例如，即時生產系統之刪除日誌顯示，為嚴格遵守資料最小化原則而進行資料刪除），控管者應向當事人說明此情況，並於技術可行的情況下，按當事人之請求提供近用，包括儲存於備份中之個人資料。例如，為使行使其權利之當事人知悉此情況，控管者得透過即時生產系統中之刪除日誌查詢，即時生產系統中剛被刪除的資料是否在備份系統中尚未被覆蓋而仍然存在。

4.2.3 The scope of a new request to access
新近用請求之範圍

109. What remains to say is that the data subject is entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request (see also 2.3.1 on the completeness of the information and 3.1.1 for the analysis of the content of the request). As a consequence, where a controller already complied with a request for access in the past and provided that the request is not excessive, the controller cannot narrow the scope of this new request. This means that in relation to any further access request of the same data subject, the

controller should not inform the data subject only on the mere changes in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to doing so. In addition, the data subject would be otherwise obliged to compile their personal data provided in order to a complete set of personal data concerning their information on the processing and on data subject rights.

另外，當事人有權對所有與其相關之資料請求近用，或對部分資料請求近用，取決於請求之範圍（另見第 2.3.1 節之資訊完整性說明及第 3.1.1 節之請求內容分析）。因此，若控管者過去已完成近用請求，且該請求非屬過度請求，控管者不得限縮新請求之範圍。亦即，就同一當事人之任何進一步近用請求而言，控管者不應僅通知當事人自上次請求以來所運用之個人資料或運用本身之單純變更，除非當事人另有明示同意。此外，當事人亦有義務對其提供之個人資料進行彙編，俾以備置關於其資料運用及當事人權利之一套完整個人資料。

4.3 Information on the processing and on data subject rights
關於運用及當事人權利之資訊

110. In addition to the access to the personal data themselves, the controller has to provide information on the processing and on data subject rights according to Art. 15(1) (a) to (h) and 15(2) GDPR. Most of the information on those specific points is already compiled, at least in general form, in the controller's record of processing activities referred to in Art. 30 GDPR and/or in its privacy notice elaborated in accordance with Art.s 12 to 14 GDPR. Therefore, it might be helpful as a first step to consult the "Guidelines on transparency under Regulation 2016/679" [59] of the Art. 29 Working Party, on the content of the information to be given under Art.s 13 and 14 GDPR.

除對個人資料本身之近用，控管者必須依據 GDPR 第 15 條第 1 項第 a-h 款及第 15 條第 2 項，提供關於運用及當事人權利之資訊。大部分關於該等具體項目之資訊均已至少以一般形式完成彙編於 GDPR 第 30 條所定之控管者運用作業紀錄，及/或 GDPR 第 12 至 14 條所定之隱私權通知中。因此，第一步先查閱第 29 條工作小組之「第 2016/679 號規則下之透明化指引」[59]，以瞭解依據 GDPR 第 13 條及第 14 條應提供之資訊內容可能會有所幫助。

111. In order to comply with Art. 15(1)(a) to (h) and 15(2), controllers may carefully use text modules of their privacy notice as long as they make sure that they are of

[59] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB"). 第 29 條工作小組之資訊，見第 WP260 號指引修訂一版，2018 年 4 月 11 日，第 2016/679 號規則下之透明化指引－經 EDPB 認可（下稱「第 29 條工作小組透明化指引（經 EDPB 認可）」）。

adequate actuality and preciseness with regards to the request of the data subject. Before or at the beginning of the data processing, some information, such as the identification of specific recipients or the specific duration of the data processing, will often only be possible in general terms. Furthermore, privacy notices as well as records of processing activities generally relate to processing concerning all data subjects and are often not tailored to the situation of a specific data subject. Some information, like for example the right to complain to a supervisory authority (see Art. 15(1)(f)), does not change depending on the person making the access request. Therefore, it may be communicated in general terms as it is also done in the privacy notice. Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is. In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored » information is the same as the « general » information. In the following, the degree of specification required is explained in relation to the individual types of information.

為遵守第 15 條第 1 項第 a-h 款及第 15 條第 2 項，控管者得謹慎使用其隱私權聲明之範本，但前提為應確保該等範本實際且正確符合當事人請求。於資料運用之前或初期，某些資訊（如特定接收方之身分或資料運用之具體時間）通常僅得透過通用文字傳達。此外，隱私權通知及運用作業紀錄通常涉及所有當事人之資料運用，通常並非專門適用特定當事人。某些資訊，例如向監管機關提出申訴的權利（見第 15 條第 1 項第 f 款），並不因近用請求之人而變更。因此，該等資訊得透過通用文字來傳達，如同隱私權通知所載。其他類型資訊（如關於接收方、類別及資料來源之資訊）可能會因提出請求之人及請求之範圍而有所不同。就第 15 條之近用請求而言，控管者所掌握的所有運用資訊可能因此必須針對其曾就該當事人所為運用作業進行更新及客製化調整。因此，援引其隱私權政策之文字並非控管者提供第 15 條第 1 項第 a-h 款及第 2 項所請求資訊之適當方式，除非「客製化」資訊與「通用」資訊相同。下文將就各類資訊說明客製化程度。

112. Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject. If the processing is carried out for several purposes, the controller has to clarify which categories of data are processed for which purpose(s). Unlike Art. 13(1)(c)

and Art. 14(1)(c), the information on the processing referred to in Art. 15(1)(a) does not contain information on the legal basis for the processing. However, as some data subjects' rights depend on the applicable legal basis, this information is important for the data subjects to verify the lawfulness of the data processing and to determine which data subject's rights are applicable in the specific situation. Therefore, in order to facilitate the exercise of data subjects' rights in line with Art. 12(2), the controller is recommended to also inform the data subject as to the applicable legal basis for each processing operation. In any event, the principle of transparent processing requires that the information on the legal bases of the processing be made available to the data subject in an accessible way (e.g. in a privacy notice).

依據第 15 條第 1 項第 a 款，目的相關資訊應針對提出請求之當事人的實際情況具體說明確切運用目的。僅列出控管者之通用目的，而未就該當事人的屆時情況說明控管者的運用目的是不夠的。若控管者有多項運用目的，則必須說明哪些類別資料是為哪些目的所運用。與第 13 條第 1 項第 c 款及第 14 條第 1 項第 c 款不同，第 15 條第 1 項第 a 款所定運用資訊不包含運用之法律依據資訊。然而，因某些當事人權利取決於適用之法律依據，該等資訊對於當事人確認資料運用之合法性及哪些情況下適用哪些當事人權利而言相當重要。因此，為依據第 12 條第 2 項促進當事人權利之行使，建議控管者亦向當事人說明各項運用作業之適用法律依據。無論如何，透明運用原則要求以便利當事人查詢的方式（例如，透過隱私權通知）向其提供運用法律依據之相關資訊。

113. Information on categories of data (Art. 15(1)(b)), in spite of the general nature of those categories and depending on the circumstances of the specific case, may also have to be tailored to the data subject's situation.

關於資料類別之資訊（第15條第1項第b款），縱令該等類別具有普遍性，並取決於具體案例之情況，可能亦必須針對當事人之情況客製化。

> **Example**: In the context of the information referred to in Art. 14, an insurer states that they process a number of categories of customer data (name, address, date of birth, telephone number, email address, bank account, pp.). If a request of access is made on the basis of Art. 15 GDPR, the data subject who makes the request must, in addition to the access to the actual data being processed (component 2), in line with Art. 15(1)(b) also be informed as to the specific categories of data which are being processed in the specific case (e.g. only e-mail address, but not the telephone number).
>
> **範例**：關於第 14 條所定資訊，一家保險公司表示其運用特定類別之客戶資料（姓名、地址、出生日期、電話號碼、電子郵件地址、銀行帳戶

等）。若近用請求係依據 GDPR 第 15 條提出，則除了向請求人提供實際運用之資料（第二個面向）外，依據第 15 條第 1 項第 b 款，亦必須說明於特定情況下運用的特定類別資料（例如，僅運用電子郵件地址，但不包括電話號碼）。

114. Information on "recipients or categories of recipients" (Article 15(1)(c)) has firstly to take into account the definition of recipients given in Art.e 4(9) GDPR. The definition of recipients is based on the disclosure of personal data to a natural or legal person, public authority, agency or other body[60]. From Art. 4 (9) GDPR follows, that public authorities acting in the framework of a particular enquiry subject to specific national provisions are not to be considered as recipients.
關於「接收方或接收方類別」之資訊（第 15 條第 1 項第 c 款），首先要考量到 GDPR 第 4 條第 9 項之接收方定義。接收方之定義是基於向自然人或法人、公務機關、機構或其他單位揭露個人資料[60]。自 GDPR 第 4 條第 9 項可知，於特定調查框架內行事且受特定國家法律拘束之公務機關，並不被視為接收方。

115. Concerning the question, if the controller is free to choose between information on recipients or on categories of recipients, it has to be recalled, that, as stated in the above-mentioned guidelines on transparency[61], already under Art. 13 and 14 GDPR information on the recipients or categories of recipients should be as concrete as possible in respect of the principles of transparency and fairness. The controller should therefore generally name the actual recipients unless it would only be possible to indicate the category of recipients. Nevertheless, sometimes naming the actual recipients is not yet possible at the time of the information under Art. 13 and 14 GDPR but only in a later stage, for example when an access request is made. The EDPB recalls in this regard, that storing information relating to the actual recipients is necessary inter alia to be able to comply with the controller's obligations under Art.s 5(2) and 19 GDPR.
關於此問題，若控管者得自由選擇提供接收方或接收方類別資訊，應注意者為，如上述關於透明化之指引所述[61]，依據 GDPR 第 13 條及第 14 條，關

[60] It should further be noted, that different controllers as defined by Article 4 (7) may exist within the same company. In this constellation a disclosure of data from one recipient to another within one company is possible. 另應注意者為，於同一公司內可能存在第 4 條第 7 項所定義之不同控管者。於此情況下，公司內之接收方可能向另一接收方揭露資料。

[61] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB"), p. 37 (Annex) 第 29 條工作小組之資訊，見第 WP260 號指引修訂一版，2018 年 4 月 11 日，第 2016/679 號規則下之透明化指引－經 EDPB 認可（下稱「第 29 條工作小組透明化指引（經 EDPB 認可）」），第 37 頁（附錄）。

於接收方或接收方類別之資訊應於透明及公平原則下盡可能具體明確。因此，除非僅能提供接收方之類別，控管者一般應提供實際接收方之名稱。然而，有時於依據 GDPR 第 13 條及第 14 條提供資料時，有可能無法提供實際接收方之名稱，而僅得於後續階段（例如於當事人提出近用請求時）始得揭露。EDPB 就此指出，為履行 GDPR 第 5 條第 2 項及第 19 條所定控管者義務，必須保存與實際接收方相關之資料。

Example: In its privacy notice an employer gives information about which categories of data are passed on to "travel agencies" or "hotels" in case of business trips, in accordance with Art. 13(1)(e) and 14(1)(e) GDPR. If an employee makes a request for access to the personal data after business trips have taken place, the employer should then, concerning the recipients of the personal data pursuant to Art. 15(1)(c), indicate in its reply the travel agency(ies) and hotel(s) that received the data. While the employer legitimately referred to categories of recipients in its privacy notice pursuant to Art. 13 and 14, because at this stage, it was not yet possible to name the recipients, it should, in line with the principles of transparency and fairness, provide information as to the specific recipients (name of travel agencies, hotels etc.) when the employee is making an access request.

範例：依據 GDPR 第 13 條第 1 項第 e 款及第 14 條第 1 項第 e 款，一雇主於其隱私權通知中說明員工出差時其特定類別資料會轉交「旅行社」或「酒店」。若員工於出差後提出近用個人資料之請求，雇主應依據第 15 條第 1 項第 c 款（就個人資料之接收方而言）於其回覆中說明收受資料之旅行社及酒店。雖然雇主依據第 13 條及第 14 條於其隱私權通知中依法說明接收方之類別，但因於此階段尚無法提供接收方名稱，其應依據透明及公平原則，於員工提出近用請求時提供確切接收方之資訊（旅行社、酒店之名稱等）。

Where a controller only provides 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[62].

在控管者僅提供接收方類別的情況下，資訊應盡可能具體明確，說明接收方之類型（亦即，揭露其從事的業務活動）、產業、領域及子領域，與接收方所在地[62]。

[62] WP29 Guidelines on transparency - endorsed by the EDPB, p. 37 (Annex)
第 29 條工作小組透明化指引（經 EDPB 認可），第 37 頁（附件）。

116. According to Art. 15(1)(d), information has to be given on the envisaged period for which the personal data will be stored, where possible. Otherwise, the criteria used to determine that period have to be provided. The information given by the controller has to be precise enough for the data subject to know how long the data relating to the data subject will continue to be stored. If it is not possible to specify the time of deletion, the duration of storage periods and the beginning of this period or the triggering event (e.g. termination of a contract, expiration of a warranty period, etc.) shall be specified. The mere reference, for example to "deletion after expiry of the statutory storage periods" is not sufficient. If the triggering event has already occurred, the specific storage period shall be indicated. Indications concerning data storage periods will have to focus on the specific data relating to the data subject. If the personal data of the data subject is subject to different deletion periods (e.g. because not all data is subject to legal storage obligations), the deletion periods shall be stated in relation to the respective processing operations and categories of data.
依據第 15 條第 1 項第 d 款，應提供個人資料保存之預計期限資訊（若可能），此外應提供用於判斷該期限之標準。控管者提供之資訊必須足夠精確，使當事人得以知悉其資料將繼續被保存多久。若無法說明刪除時間，則應說明保存期間及該等期間之起始或觸發事件（如合約之終止，保固期之屆滿等）。舉例而言，僅提及「於法定保存期間終了後刪除」是不夠的。若已發生觸發事件，則應說明具體的保存期限。關於資料保存期限之資訊必須具體適用當事人相關資料。若當事人之個人資料受制於不同的刪除時限（例如，因並非所有資料均受法定保存義務所拘束），則應就各項運用作業及資料類別說明適用之刪除時限。

117. Whereas information on the right to lodge a complaint with a supervisory authority (Art. 15 (1) (f)) is not dependant on the specific circumstances, the data subjects rights mentioned in Art. 15 (1) (e) vary depending on the legal basis underlying the processing. With regard to its obligation to facilitate the exercise of data subject rights pursuant to Art. 12(2), the response by the controller on those rights shall be individually tailored to the case of the data subject and relate to the processing operations concerned. Information on rights that are not applicable for the data subject in the specific situation should be avoided.
當事人有權向監管機關提出申訴（第 15 條第 1 項第 f 款）之相關資訊不會因具體案件情況而有變更，而第 15 條第 1 項第 e 款所定當事人權利則會因運用之法律依據而有不同。關於控管者依據第 12 條第 2 項促進當事人行使權利之義務，控管者對該等請求之回覆，應針對當事人個別情況及與其相關之運用作業進行調整。應避免提供不適用當事人具體情況的相關權利資訊。

118. According to Art. 15(1)(g), "any available information" as to the source of the data has to be provided, where the personal data are not collected from the data subject. The degree of available information may change over time.
依據第 15 條第 1 項第 g 款，若個人資料並非自當事人處所蒐集，即必須提供關於資料來源之「任何可用資訊」。可用資訊之範圍可能會隨時間而有所變化。

Example: The privacy policy of a large company states:
範例：一家大公司之隱私權政策指出：

"Credit checks help us to prevent problems in payment transactions. They guarantee the protection of our company against financial risks, which can also affect sales prices in the medium to long term. A credit check is necessarily carried out when we are going to ship goods without receiving the respective purchase price at the same time, e.g. in the case of a purchase on account. Without carrying out the credit check, only a prepayment payment option (immediate bank transfer, online payment provider, credit card) is possible.
「信用調查協助本公司防範付款問題，確保本公司免受金融風險影響，該等風險會影響中長期銷售價格。當本公司於尚未同時收到相應買賣價金的情況下出貨時（例如允許客戶賒帳時），就必須進行信用調查。若不進行信用調查，僅能選擇預付款項（即時銀行轉帳、線上支付、信用卡等）。

For the purpose of credit checking, we will send your name, address and date of birth to the following service providers, for example: (1) Financial information agency X (2) Business Information Provider Y, (3) Commercial Credit Reference Agency Z.
為進行信用調查，本公司會將您的姓名、地址及出生日期發送予以下服務供應商，例如：(1) 金融資訊機構 X；(2) 企業資訊供應商 Y；(3) 商業信用資訊機構 Z。

The data are passed on to the above-mentioned credit institutions only within the scope of what is legally permissible and only for the purposes of the analysis of your past payment behaviour as well as for the assessment of the risk of default on the basis of mathematical-statistical procedures using address data as well as for verification of your address (examination of delivery). Depending on the result of the credit check, we may no longer be able to offer you individual payment methods, such as the purchase of invoices."
該等資料僅會在法律允許之範圍內提供予上述信用機構，且僅會用於分

析您過去的付款行為，於數學統計程序的基礎上評估違約風險，及採用地址資料查驗您的地址（交貨確認）。依據信用調查結果，本公司可能無法向您提供特定付款方式（如開立發票後付款）。

The privacy notice thus contains general information on the possibility of obtaining information from the listed Economic Information Offices in accordance with Art. 13 and 14. If it is not clear ex ante, which of the companies will get involved in the processing, it is sufficient to mention the names of the eligible companies in the privacy policy. In the context of a request based on Art. 15, in addition to the information that a creditworthiness information has been obtained, it would then (ex post) be necessary to disclose, which of the companies mentioned has been involved exactly. It is clearly expressed by Art. 15(1)(g), that information on the processing of the data comprise "any available information as to their source" where the personal data are not collected from the data subject.

因此，隱私權通知包含依據第 13 條及第 14 條可能自經濟資訊辦公室取得資訊之一般資訊。若事前不清楚哪些公司將參與運用，則於隱私權政策中提供符合條件之公司名稱就足夠；若當事人依據第 15 條提出請求，除說明已取得信用資訊外，亦必須（事後）揭露哪些公司參與信用調查。第 15 條第 1 項第 g 款明示規定，若個人資料並非自當事人處蒐集，則資料運用資訊包括「任何關於其來源之可用資訊」。

119. Art. 15(1)(h) provides that every data subject should have the right to be informed, in a meaningful way, inter alia, about the existence and underlying logic of automated decision-making including profiling concerning the data subject and about the significance and the envisaged consequences that such processing could have[63]. If possible, information under Art. 15(1)(h) has to be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access.

第 15 條第 1 項第 h 款規定，所有當事人均應有權以有意義的方式被告知自動化決策之存在及基本邏輯，包括關於當事人之剖析，及此等運用的可能意義及預期結果[63]。若可能，第 15 條第 1 項第 h 款所定資訊必須更加具體明確，說明對請求近用之當事人作出具體決策的理由。

120. Information about intended transfers of data to a third country or an international

[63] See on this behalf Guidelines on transparency under Regulation 2016/679 (WP 260), para. 41, with reference to Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251).
見 2016/679 號規則下之透明化指引（WP260），第 41 段，參考 2016/679 號規則中關於自動化個人決策及剖析之指引（WP251）。

organisation, including the existence of a Commission adequacy decision or suitable safeguards, has to be given under Art. 13(1)(f) and 14(1)(f). In the context of a request for access under Art. 15, Art. 15(2) requires information on the appropriate safeguards pursuant to Art. 46 only in cases where transfer to a third country or an international organisation is actually taking place.
依據第 13 條第 1 項第 f 款及第 14 條第 1 項第 f 款，必須提供關於擬向第三國或國際組織移轉資料之資訊，包括是否存在經歐盟執委會認定之適足性或適當之保護措施。就第 15 條所定之近用請求而言，第 15 條第 2 項規定，僅有在實際向第三國或國際組織進行移轉的情況下，始得提供其依據第 46 條實施適當保護措施之資訊。

5 HOW CAN A CONTROLLER PROVIDE ACCESS?
控管者如何提供近用？

121. The GDPR is not very prescriptive as to how the controller has to provide access. The right of access may be easy and straight forward to apply in some situations, for example when a small organisation holds limited information about the data subject. In other situations, the right of access is more complicated because the data processing is more complex; with regard to the number of data subjects, the categories of processed data as well as the flow of data within and between different organisations. Considering the differences in personal data processing, the appropriate way to provide access may vary accordingly.
GDPR 對控管者如何提供近用的問題並未設定明確規範。近用權的適用於特定情況下可能很簡單也很直覺，例如，在小型組織所持有當事人資料較為有限的情況下。於其他情況下，資料運用（就當事人數量、被運用資料類別及資料於不同組織內部及之間流動而言）若較為複雜，近用權亦會較為複雜。考量到個人資料運用之差異，提供近用的適當方式可能也會因此有所不同。

122. This section aims at giving some guidance and practical examples on different ways for controllers to comply with an access request as well as to the meaning of Art. 12(1) in relation to the right of access. This section will also give some guidance about what is considered to be a commonly used electronic form, as well as the timing for the provision of access under Art. 12(3).
本節旨在就控管者遵守近用請求的不同方式，及第 12 條第 1 項與近用權相關之涵義，提供一些指引及實際範例。本節亦將針對一般認為常用的電子表單及依據第 12 條第 3 項提供近用之時間提供指引。

5.1 How can the controller retrieve the requested data?
控管者如何檢索當事人請求的資料？

123. The data subjects should have access to all the information that the controller processes regarding them. This means, for example, that the controller is obliged to search for personal data throughout its IT systems and non-IT filing systems. When carrying out such search, the controller should use available information in the organisation regarding the data subject that likely will result in matches in the systems depending on how the information is structured[64]. For example, if the information is sorted in files depending on name or a reference number, the search could be limited to these factors. But if the structure of the data depends on other factors, such as family relations or professional titles or any kind of direct or indirect identifiers (e.g. customer number, user name or IP-addresses), the search needs to be extended to include these, provided that the controller also holds this information related to the data subject, or is provided with that information by the data subject. The same applies when records regarding third persons are likely to contain personal data regarding the data subject. The controller may, however, not require the data subject to provide more information than necessary to identify the data subject.

當事人應有權近用其被控管者運用的所有資訊。舉例而言，這表示控管者有義務於其資訊科技（IT）系統及非資訊科技（non-IT）歸檔系統中搜尋個人資料。於進行該等搜尋時，控管者應依據資料架構，使用組織中可能會因此於系統中產生配對結果的當事人可用資訊 [64]。例如，若資訊係依據姓名或參照號碼於檔案中分類，則應依據該等因素進行搜尋。然而，若資料架構取決於其他因素，如家庭關係或專業職稱或任何類型的直接或間接識別碼（如客戶號碼，使用者名稱或 IP 位址），就應該依據該等因素進行搜尋，但前提為控管者持有與當事人相關之該等資訊，或當事人有提供該等資訊。前述同樣適用於第三人紀錄可能包含當事人個人資料的情況。然而，控管者不得要求當事人提供超出識別當事人所必須之資訊。

124. In line with Art. 25 GDPR on data protection by design and by default, the controller should also already have implemented functions enabling the compliance with data subject rights. This means, in this context, that there should be appropriate ways to find and retrieve information regarding a data subject when handling a request. However, it should be noted that an excessive interpretation in this regard could lead to functions for finding and retrieving information that in itself pose a risk for the privacy of data subjects. It is therefore important to keep in mind that the process to retrieve data should also be designed in a data protection friendly way, so that it doesn't compromise the privacy of others, for example the employees of the controller.

[64] Such a search should naturally also include information that is held by a processor, see. Article 28(3)(e). 此等搜尋自然亦應包括受託運用者所掌握之資訊，見第 28(3)(e)條。

依據 GDPR 第 25 條關於資料保護設計及預設規定，控管者亦應已建置得以遵守當事人權利之功能。亦即，於此情況下，於處理請求時，應有適當方式可以搜尋及檢索關於當事人之資訊。然而，應注意者為，於此方面之過度解釋可能會導致搜尋及檢索資訊之功能本身對當事人隱私構成風險。因此重要的是應注意檢索資料的流程亦應以資料保護友善的方式設計，以避免損害他人（例如控管者的員工）隱私。

5.2 Appropriate measures for providing access
提供近用之適當措施

5.2.1 Taking "appropriate measures"
採取「適當措施」

125. Art. 12 GDPR lays down the requirements for providing access, i.e. for providing the confirmation, the personal data and the supplementary information under Art. 15, and specifies also the form, manner and time limit in relation to the right of access. Art. 29 Working Party's "Guidelines on transparency under Regulation 2016/679"[65] provides further guidance as regards Art. 12, mostly in relation to Art. 13 and 14 but also in relation to Art. 15 and on transparency in general. Thus, what is defined in those guidelines can often equally apply with regards to providing access under Article 15.
GDPR 第 12 條規定提供近用之要件，亦即，依據第 15 條提供確認、個人資料及補充資訊，並規定行使近用權之形式、方法與時間限制。第 29 條工作小組「第 2016/679 號規則下之透明化指引」[65] 提供第 12 條的進一步指導，主要係關於第 13 及 14 條，但亦涉及第 15 條及透明化之一般議題。因此，該指引所提供之定義通常可同樣適用於第 15 條所定近用之提供。

126. Art. 12(1) of the GDPR states that the controller shall take appropriate measures to provide any communication under Art. 15 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Art. 12(2) provides that the controller shall facilitate the data subject's exercise of access right. The more precise requirements in this regard will have to be assessed case by case. When deciding which measures are appropriate, the controllers have to take into account all the relevant circumstances, including, but not limited to, the amount of data being processed, the complexity of their data processing and the knowledge they have about their data subjects, for

[65] Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB"). 第 29 條工作小組之資訊，見第 WP260 號指引修訂一版，2018 年 4 月 11 日，第 2016/679 號規則下之透明化指引－經 EDPB 認可（下稱「第 29 條工作小組透明化指引（經 EDPB 認可）」）。

example if the majority of the data subjects are children, elderly people or people with disabilities. In addition, in situations where the controller is made aware of any special needs for the data subject making the request, for example through additional information in the request made, the controller needs to take these circumstances into consideration. As a result the appropriate measures will vary.
GDPR 第 12 條第 1 項規定，控管者應採取適當措施，以簡明、透明、可理解及易近用之形式，採用清晰及簡明之語言，向當事人提供第 15 條下關於運用之任何資訊。第 12 條第 2 項規定，控管者應使當事人方便行使近用權。這方面更精確的要求則必須視個案情況進行評估。在決定哪些措施具適當性時，控管者必須考量到所有相關情況，包括但不限於正在運用的資料量、其資料運用之複雜性及其對當事人之瞭解，例如，若當事人大多數是兒童、老人或殘疾人士的情況。此外，於控管者被告知當事人有任何特殊需求的情況下（例如透過請求中之額外資訊告知），控管者應將該等情況考量在內。因此，適當措施會視個案而有所不同。

127. It is important to keep in mind when making the assessment that the term "appropriate" should never be understood as a way of limiting the scope of the data covered by the right of access. The term "appropriate" does not mean that the efforts to provide the information can be balanced against, for example, any interest the data subject may have in obtaining the personal data. Instead the assessment should aim at choosing the most appropriate method for providing all information covered by this right, depending on the specific circumstances in each case. As a consequence, a controller who processes a vast amount of data on a large scale must accept to undertake great efforts to ensure the right of access to the data subjects in a concise, transparent, intelligible and easily accessible form, by using plain and clear language.
應注意於進行評估時，必須確保「適當」一詞不應被理解為限縮近用權所涵蓋的資料範圍。「適當」一詞並不代表控管者在提供資訊方面所作努力得與例如當事人在取得個人資料方面的任何利益等面向進行權衡。實則，評估之目的應係依據各案件之具體情況，選擇最適當方法來提供此權利所涵蓋的所有資訊。因此，大規模運用大量資料之控管者必須同意付出大量努力，以確保近用權得以簡明、透明、可理解及易近用之形式，透過簡明且清晰的語言向當事人提供。

128. It needs to be avoided to direct the data subject to different sources in response to a data access request. As previously stated in the WP29 Guidelines on Transparency (with regard to the notion of "provide" in Art. 13 and 14), the notion of "provide" entails that *"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"[66]. Therefore, and in respect of the transparency principle, data subjects must obtain from the controller the information and personal data required by Art. 15(1), 15(2) and 15(3) in a way that enables a complete access to the requested information. The method chosen by the controller must, in line with that, be one that actually provides the data subject with the requested data and information, hence it would not be considered appropriate to solely refer the data subject to check the requested data stored on their own device, for example to check clickstream history and IP addresses on their mobile phone.

應避免在回覆近用權請求時請當事人參考不同資料來源。如先前於第 29 條工作小組透明化指引（關於第 13 條及第 14 條中「提供」之概念）所述，「提供」之概念代表「*不應要求當事人自行於其他資訊（如網站或應用程式之使用條款及條件）中搜尋此等條款所涵蓋之資訊*」[66]。因此，就透明化原則而言，當事人必須自控管者處取得第 15 條第 1 項、第 15 條第 2 項及第 15 條第 3 項所定資訊及個人資料，其方式應能使當事人完整近用所請求之資訊。依據上述要求，控管者所選擇的方法必須是能真正向當事人提供所請求資料及資訊之方法，因此，舉例而言，僅要求當事人自行查詢儲存於其自身裝置上的所請求資料（例如查詢其手機上之點擊紀錄及 IP 位址）並非適當作法。

129. In accordance with the accountability principle, a controller must document their approach to be able to demonstrate how the means chosen to provide the necessary information under Art. 15 are appropriate in the circumstances at hand.

依據課責性原則，控管者必須記錄其做法，俾以證明其為提供第 15 條所定必要資訊而選擇的方法，在當前情況下屬適當作法。

5.2.2 Different means to provide access
提供近用的不同方式

130. As already explained in section 2.2.2 above, when making an access request the data subjects are entitled to receive a copy of their data undergoing processing pursuant to Art. 15(3) together with the supplementary information, which is considered as the main modality for providing access to the personal data.

如上文第 2.2.2 節所述，當事人於提出近用請求時，有權依據第 15 條第 3 項取得一份控管者正在運用其資料之複製本及補充資訊，這被認為是提供個人資料近用的主要方式。

131. However, under some circumstances it could be appropriate for the controller to

[66] WP29 Guidelines on transparency - endorsed by the EDPB, para. 33.
第 29 條工作小組透明化指引（經 EDPB 認可），第 33 段。

provide access through other ways than providing a copy. Such non-permanent modalities of access to the data could be, for example: oral information, inspection of files, onsite or remote access without possibility to download. These modalities may be appropriate ways of granting access for example in cases where it is in the interest of the data subject or the data subject asks for it. Non-permanent ways of access can be sufficient and adequate in certain situations; for example, it can satisfy the need of the data subjects to verify that the data in the record are correct by giving them a chance to have a glance at the original record. A controller is not obliged to provide the information through other ways than providing a copy but should take a reasonable approach when considering such a request. Nor does giving access through other ways than providing a copy preclude the data subjects from the right to also have a copy, unless they recognisably waived this right.
然而，於特定情況下，控管者透過提供複製本以外之其他方式提供近用可能亦屬適當作法。該等非永久性之資料近用方式包括，例如：口頭資訊、文件閱覽、現場或遠距近用（未提供下載）。該等方式可能屬於授予近用的適當方式，例如於符合當事人利益或當事人要求的情況下。於特定情況下，非永久性之近用方式亦屬充分、適當；例如，使當事人有機會閱覽原始紀錄，以滿足當事人查驗紀錄所載資料是否正確的需求。控管者無義務透過提供複製本以外之其他方式提供資訊，但於考量該等請求時應採取合理作法。透過提供複製本以外之其他方式提供近用，亦不排除當事人亦有取得複製本之權利，除非其明示拋棄這項權利。

132. The controller may choose, depending on the situation at hand, to provide the copy of the data undergoing processing, together with the supplementary information, in different ways, e.g. by e-mail, physical mail or by the use of a self-service tool. In any case, the controller has to consider appropriate technical and organizational measures, including adequate encryption when providing information via e-mail or online-self-service tools.
控管者得依據實際情況，選擇以不同方式提供其正在運用資料之複製本及補充資訊，例如透過電子郵件、實體郵件或使用自助服務工具。無論如何，控管者均必須考量採取適當的技術性及組織性措施，包括於透過電子郵件或線上自助工具提供資訊時進行適當加密。

133. In the situation, where the controller is processing personal data regarding the person making the request only in a small scale, the copy of the personal data and the supplementary information can and should be provided through a rather simple procedure.
於此情況下，若控管者僅是小規模地運用請求人的個人資料，個人資料之複製本及補充資訊可以且應該透過較為簡單的程序提供。

Example 1: A local bookstore keeps a record of name and addresses of their customers that have ordered home delivery. A customer visits the bookstore and makes a request for access. In this situation it would be sufficient to print out the personal data concerning the customer directly from the business system, while also supplying the supplementary information in Art. 15(1) and (2).
範例 1：一家當地書店保留一份曾購買送貨到府商品客戶之姓名及地址紀錄。一名客戶來到書店提出近用請求。於此情況下，直接自業務系統中列印出客戶個人資料並提供第15條第1項及第2項之補充資訊即已足夠。

Example 2: A monthly donor to a charity organisation makes an access request through e-mail. The charity organisation holds information about donations made in the past twelve months, as well as names and e-mail addresses of the donors. The controller could provide the copy of the personal data and the supplementary information by responding to the e-mail, provided that all necessary safeguards are applied, taking into consideration for example the nature of the data.
範例 2：某慈善組織之每月捐款人透過電子郵件提出近用請求。該慈善組織持有過去 12 個月的捐款資訊，及捐款人姓名及電子郵件地址。控管者得透過回覆電子郵件的方式提供個人資料之複製本及補充資訊，但必須在考量資料性質等因素後採用所有必要之保護措施。

134. Even controllers that process a vast amount of data can choose to rely on manual routines for handling access requests. If the controller processes data in several different departments, the controller needs to collect the personal data from each department to be able to respond to the data subject request.
即使是運用大量資料之控管者亦得選擇透過手動（人工）程序來處理近用請求。若控管者有若干部門運用資料，控管者應自各部門蒐集個人資料，俾以回應當事人之請求。

Example: An administrator is appointed by the controller to handle the practical issues regarding access requests. When receiving a request the administrator sends an enquiry through e-mail to the different departments of the organisation asking them to collect personal data regarding the data subject. Representatives of each department give the administrator the personal data processed by their department. The administrator then sends all the personal data to the data subject

together with the necessary supplementary information, for example and when appropriate, by e-mail.
範例：控管者指定一行政人員來處理關於近用請求的實務問題。當收到請求時，該行政人員透過電子郵件向該組織之不同部門發出詢問，要求其蒐集關於該當事人之個人資料。各部門代表向該行政人員提供其部門所運用之個人資料。該行政人員隨後將所有個人資料連同必要的補充資訊（若適用）透過電子郵件發送予當事人。

135. Although manual processes for handling access requests could be regarded as appropriate, some controllers may benefit from using automated processes to handle data subject requests. This could for example be the case for controllers that receive a large number of requests. One way to provide the information under Art. 15 is by providing the data subject with self-service tools. This could facilitate an efficient and timely handling of data subjects' requests of access and will also enable the controller to include the verification mechanism in the self-service tool.
雖然透過手動（人工）程序處理近用請求得被認為適當，但一些控管者可能會因採用自動程序來處理當事人請求而受益。例如，對收到大量請求的控管者而言，就可能如此。依第 15 條規定提供資訊的方法之一是為當事人提供自助服務工具，此得促使有效及迅即處理當事人之近用請求，亦得使控管者於自助服務工具中加入查驗機制。

Example: A social media service has an automated process for handling access requests in place that enables the data subject to access their personal data from their user account. To retrieve the personal data the social media users can choose the option to "Download your personal data" when logged into their user account. This self-service option allows the users to download a file containing their personal data directly from the user account to their own computer.
範例：某社群媒體服務有自動處理近用請求之程序，使當事人能夠自其使用者帳戶中近用其個人資料。為檢索個人資料，社群媒體使用者得於登入其使用者帳戶時選擇「下載您的個人資料」選項。此自助選項讓使用者得直接自使用者帳戶中下載包含其個人資料的檔案至其電腦中。

136. The use of self-service tools should never limit the scope of personal data received. If not possible to give all the information under Art. 15 through the self-service tool, the remaining information needs to be provided in a different manner. The controller may indeed encourage the data subject to use a self-service tool that the controller has set in place for handling access requests. However, it should be reminded that the controller must also handle access requests that are not sent

through the established channel of communication[67].
使用自助服務工具絕不應限制所提供個人資料之範圍。若無法透過自助服務工具提供第 15 條規定所有資訊，則需要透過其他方式提供其餘資訊。控管者確實得鼓勵當事人使用控管者為處理近用請求而提供的自助服務工具。然而，應注意者為，控管者亦必須處理未採用其指定聯絡管道所提出的近用請求[67]。

5.2.3 Providing access in a "concise, transparent, intelligible and easily accessible form using clear and plain language"
以「簡明、透明、可理解及易近用之形式，使用清晰及簡明之語言」提供近用

137. According to Art. 12(1) the controller shall take appropriate measures to provide access under Art. 15 in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
依據第 12 條第 1 項，控管者應採取適當措施，以簡明、透明、可理解及易近用之形式，使用清晰及簡明之語言提供第 15 條所定之近用。

138. The requirement that providing access to the data subject has to be done in a concise and transparent form means, that controllers should present the information efficiently and succinctly in order to be easily understood and captured by the data subject, especially if it is a child. The controller needs to take into account the quantity and complexity of the data when choosing means for providing access under Art. 15.
向當事人提供近用必須以簡明且透明之形式完成，亦即，控管者應有效且簡明地呈現資訊，使當事人容易理解及掌握，特別是當事人為兒童的情況。控管者於選擇依第 15 條所定提供近用的方式時，需要考量到資料的數量及複雜性。

> **Example**: A social media provider processes a vast amount of information about a data subject. A large part of this personal data is information contained in hundreds of pages of log files where the data subject's activities on the website are registered. If data subjects request access to their personal data, these log files are indeed covered by the right of access. The right of access may therefore be formally fulfilled if these hundreds of pages of log files were to be provided to the data subject. However, without measures taken to facilitate the understanding of the log files, the data subject's right of access might not be met

[67] See section 3.1.2.
見 3.1.2 節。

in practice, because no knowledge can easily be drawn from the log files, therefore not fulfilling the requirement of Art. 12(1). The controller must therefore be careful and thorough when choosing the way the information and personal data is presented to the data subject.

範例：社群媒體提供者運用大量當事人資料。該等個人資料中很大一部分是包含於數百頁日誌文件中的當事人網站活動紀錄資訊。若當事人請求近用其個人資料，該等日誌文件確實屬於近用權之範圍。因此，若將這幾百頁之日誌文件提供予當事人，近用權可能會在形式上獲得滿足。然而，若不採取措施促使當事人瞭解該等日誌文件，當事人之近用權可能在實際上無法獲得滿足，因為當事人可能無法輕易理解日誌文件之意義，因此不符合第 12 條第 1 項之要求。因此，控管者於選擇向當事人呈現資訊及個人資料之方式時，必須謹慎、周全。

139. Under the circumstances in the example above, the use of a layered approach, similar to the layered approach advocated in the Guidelines on transparency with regard to privacy notices[68], could be an appropriate measure to fulfil both the requirements in Art. 15 and 12(1). This will be further developed under section 5.2.4. below. The requirement that the information is "intelligible" means that it should be understood by the intended audience[69], whilst keeping in mind any special needs that the data subject might have that is known to the controller[70]. Since the right of access often enables the exercise of other data subject rights, it is crucial that the information provided is made understandable and clear. This is because data subjects will only be able to consider whether to invoke their right to, for example, rectification under Art. 16 once they know what personal data are being processed, for what purposes etc. As a result, the controller might need to supply the data subject with additional information that explains the data provided. It should be emphasised that the complexity of data processing puts an obligation on the controller to provide the means to make the data understandable and could not be used as an argument to limit the access to all data. Similarly, the obligation on the controller to provide data in a concise manner cannot be used as an argument to limit access to all data.

於上述範例情況下，使用分層方法（類似於透明化指引針對隱私權通知所

[68] WP29 Guidelines on transparency - endorsed by the EDPB, para. 35.
第 29 條工作小組透明化指引（經 EDPB 認可），第 35 段。

[69] Intelligibility is closely linked to the requirement to use a plain and clear language (WP29 Guidelines on transparency - endorsed by the EDPB, para. 9). What is said about a plain and clear language in para. 12-16 with regards to information referred to in Articles 13 and 14, equally applies to communication under Article 15.
可理解性與使用簡明、清晰語言之要求密切相關（第 29 條工作小組透明化指引（經 EDPB 認可），第 9 段）。第 12-16 段中關於第 13 條及第 14 條所定資訊之規範，同樣適用第 15 條所定資訊。

[70] See para. 126.
見第 126 段。

建議採用的分層方法[68]），可能屬適當措施，可滿足第 15 條及第 12 條第 1 項之要求。此點將於以下第 5.2.4 節進一步說明。資訊「可理解」之要求係指其應被目標受眾所理解[69]，同時應考量控管者已知之當事人特殊需求[70]。因近用權通常能使當事人行使其他權利，因此提供之資訊必須為可理解且清晰，因為當事人只有在知悉哪些個人資料被運用及運用目的等資訊後，始得考量是否行使其相關權利，例如第 16 條所定之更正權。因此，控管者可能需要向當事人提供額外資訊，以就所提供之資料進行說明。應強調者為，資料運用之複雜性使控管者有義務以可理解的方式提供資料，但這不能作為限制近用所有資料的理由。同樣地，控管者有義務以簡明的方式提供資料，這也不能作為限制近用所有資料的理由。

Example: An ecommerce website collects data about items viewed or purchased on its website for marketing purposes. A part of this data will consist of data in a raw format[71], which has not been analysed and may not be directly meaningful to the reader (codes, activity history etc.). Such data related to the data subjects activities is also covered by the right of access and should as a consequence be provided to the data subject upon access request. When providing data in a raw format it is important that the controller takes the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user friendly form. Also, it could in such a document be explained that abbreviations and other acronyms for example "A" means that the purchase has been interrupted and "B" means that the purchase has gone through.

範例：電子商務網站為行銷目的蒐集當事人於其網站上瀏覽或購買商品之資料。該等資料之一部分包括原始格式之資料[71]，該等資料未經分析，可能對讀者沒有直接意義（代碼、活動紀錄等）。這類與當事人活動相關之資料亦屬於近用權之範圍，因此應於接獲近用請求時提供予當事人。於提供原始格式之資料時，控管者必須採取必要措施來確保當事人理解該等資料，例如提供一份解釋性文件，將原始格式翻譯成使用者可理解的形式。另外，也可在該等文件中說明簡寫及縮寫用語之意義，例如「A」代表著交易中斷，「B」代表交易已完成。

[71] The raw data could be explained as unanalysed data underlying a processing. Raw data could exist on different levels, where the lowest level of data may only be machine-readable (such as "bits"). It should be stressed that the information provided to the data subject always must be in a human readable format. 原始資料得被解釋為資料運用中未經分析之資料。原始資料得存在於不同層次，其中最低層次之資料可能僅包含機器可讀資料（如「位元」）。應該強調者為，提供予當事人之資訊永遠必須屬人類可讀之格式。

140. The “easily accessible” element means that the information under Art. 15 should be presented in a way that is easy for the data subject to access. This applies for example, to the layout, appropriate headings and paragraphing. The information should always be given in a plain and clear language. A controller that offers a service in a country should also offer answers in the language that is understood by the data subjects in that country. The use of standardised icons is also encouraged when it facilitates the intelligibility and accessibility of the information. When the request for information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information, the controller is expected to take measures facilitating the understanding of the information provided, including oral information when adequate[72]. The controller should take special care to ensure that people with special needs, such as elderly people, children, visually impaired persons or persons with cognitive disabilities can exercise their rights, for instance by proactively providing easily accessible elements to facilitate exercise of these rights.

「易近用」之要件係指第 15 條所定資訊應以一種容易使當事人近用之方式呈現。例如資料之排版、適當標題及段落皆有適用。資訊應永遠以簡明及清晰之語言提供。於某國家提供服務之控管者，亦應以該國當事人所理解之語言提供回覆。若使用標準化圖示有利於資訊之可理解性及可近用性，亦鼓勵使用該等圖示。當資訊請求涉及視力受損之當事人或其他於近用或理解資訊方面可能有困難之當事人時，控管者應採取措施促進對所提供資訊之理解，包括於適當情況下提供口頭資訊 [72]。控管者應特別注意確保有特殊需要之人，如老人、兒童、視力受損之人或有認知障礙之人均得以行使其權利，例如主動提供易近用之管道，以促使該等權利之行使。

5.2.4 A vast amount of information necessitates specific requirements on how the information is provided
需提供大量資訊時之方式的具體規範

141. Regardless of the means used to provide access there may be a tension between the amount of information the controller needs to provide data subjects with and the requirement that it must be concise. One way of achieving both, and an example of an appropriate measure for certain controllers, when a vast amount of data is to be provided, is to use a layered approach. This approach can facilitate the data subjects’ understanding of the data. It should nevertheless be stressed that this approach can only be used under certain circumstances and needs to be carried out in a way that does not limit the right of access, as explained below. Furthermore,

[72] See WP29 Guidelines on transparency - endorsed by the EDPB, para. 21.
見第 29 條工作小組透明化指引（經 EDPB 認可），第 21 段。

the use of a layered approach should not create an extra burden for the data subject. Hence, it would be best suited when access is provided in an online context. A layered approach is merely a way to present the information under Art. 15 in a manner which is also compliant with the requirements in Art. 12(1) and should not be confused with the possibility for the controllers to request that the data subject specifies the information or processing activities to which the request relates, as prescribed in Recital 63[73].

無論用什麼方式提供近用，在控管者需要提供給當事人的資訊量及要求其必須簡明這兩者之間可能存在矛盾。於需要提供大量資料的情況下，實現這兩者的方法，以及特定控管者實施適當措施的範例，就是採用分層方法。此等方法得促進當事人對資料之理解。惟應強調者為，此等方法僅得於特定情況下使用，且需要於不限制近用權的情況下實施，此點將於下文說明。此外，分層方法之使用不應該給當事人帶來額外負擔。因此，當於線上提供近用時，此方法為最適當作法。分層方法僅是一種以符合第 12 條第 1 項規範的方式呈現第 15 條所定資訊之方式，而不應與前言第 63 段[73]所載控管者要求當事人具體說明其請求所涉資訊或運用作業之可能性混為一談。

142. A layered approach in relation to the right of access means that a controller, under certain circumstances, can provide the personal data and the supplementary information required under Art. 15 in different layers. The first layer should include information about the processing and data subject's rights according to Art. 15(1)(a)-(h) and 15(2) as well as a first part of the processed personal data. In a second layer, more personal data should be provided.

與近用權相關之分層方法係指控管者於特定情況下得分層提供第 15 條所定個人資料及補充資訊。第一層應包括關於運用及當事人依據第 15 條第 1 項第 a-h 款及第 15 條第 2 項所享有權利之資訊，以及所運用個人資料之第一部分。第二層則應提供更多個人資料。

143. When deciding what information should be given in the different layers the controller should consider what information the data subject in general would consider as most relevant. In line with the fairness principle, the first layer should also contain information on the processing which has the most impact on the data subject and processing which could surprise them[74]. The controllers need to be able to demonstrate accountability as to their reasoning of the above.

當決定於不同階層中應該提供哪些資訊時，控管者應該考量哪些資訊是當事人一般會認為屬最相關者。依據公平原則，第一層亦應包含對當事人影

[73] See also section 2.3.1.
另見 2.3.1 節。

[74] See WP29 Guidelines on transparency - endorsed by the EDPB, para. 36.
見第 29 條工作小組透明化指引（經 EDPB 認可），第 36 段。

響最大之運用資訊，及可能使其感到意外的運用資訊[74]。控管者應能對上述運用之理由展現課責性。

Example: A controller analyses big data sets to place customers in different segments depending on their online behaviour. In this situation, it can be assumed that the information that is the most important for the data subjects to obtain is information about what segment they have been put in. As a result, this information should be included in the first layer. The data in a raw format[75] that has not yet been analysed or further processed, such as user activity on a website, is also personal data covered by the right of access, however, it could in some cases be sufficient to provide this information in another layer.

範例：控管者分析大數據集，依據客戶之線上行為將其歸納至不同子市場。於此情況下可假設，對當事人而言，最重要的資訊係其被歸納至哪個子市場之資訊。因此，該等資訊應屬第一層資訊。未經分析或進一步運用之原始格式資料[75]，如使用者於網站上的活動，亦屬近用權所涵蓋之個人資料；然而，在特定情況下，於其他層級提供該等資訊即屬足夠。

144. For the use of layered approach to be considered as an appropriate measure it is necessary that the data subject is informed at the outset that the information under Art. 15 is structured into different layers and provided with a description of what personal data and information that will be contained in the different layers. In this way it will be easier for the data subject to decide what layers they want to access. The description should objectively reflect all the categories of personal data that are actually processed by the controller. It also needs to be clear how the data subject can get access to the different layers. Access to the different layers shall not entail any disproportionate effort for the data subject and shall not be made conditional to the formulation of a new data subject request. This means that the data subjects must have the possibility to choose whether to access all layers at once or if they would be satisfied with only accessing one or two of the layers.

為使分層方法之使用被認為屬適當措施，有必要從一開始就告知當事人，第 15 條所定資訊將被分為不同層級提供，並提供關於不同層級將包含哪些個人資料及資訊之說明。這樣一來，當事人就會更容易決定要近用哪些層級資訊。該說明應客觀地反映控管者實際運用之所有類別個人資料，亦須清楚說明當事人可如何近用不同層級資訊。近用不同層級資訊不應使當事人作出任何不成比例之付出，亦不應以當事人提出新的請求為條件。亦即，當事人必須有可能選擇是否一次近用所有層級資訊，或其是否接受僅近用

[75] See footnote 71.
見註腳 71。

其中一個或兩個層級資訊。

Example: A data subject makes an access request to a video streaming service. The request is made through an option that is available when data subjects have logged into their account. The data subject is presented with two options, appearing as buttons on the webpage. Option one is to download part 1 of the personal data and the supplementary information. This contains, for example a recent streaming history, account information and payment information. Option two is to download part 2 of the personal data that contains technical log files about the data subjects activities and historical information on the account. In this case, the controller, has made it possible for data subjects to exercise their right in a way that does not create an extra burden for the data subject.
範例：當事人向影片串流服務提出近用請求。此請求是透過當事人在登入其帳戶後即可使用的選項所提出。當事人可透過網頁上的按鈕選擇兩個選項。選項一是下載個人資料之第一部分及補充資訊，這包括例如最近的串流紀錄、帳戶資訊及付款資訊。選項二是下載個人資料之第二部分，其中包含關於當事人活動之技術日誌檔案及帳戶之歷史資訊。於此情況下，控管者已使當事人有可能以一種不會讓當事人造成額外負擔的方式來行使其權利。

Situation 1: In cases where the data subject only chooses the button to download part 1 of the personal data, the controller is obliged only to provide part 1 of the data.
情況 1：當事人僅選擇下載個人資料第一部分之按鈕時，控管者有義務僅提供資料之第一部分。

Situation 2: In cases where the data subject chooses the buttons for both part 1 and part 2 of the data, the controller cannot communicate only part 1 of the data and ask for a new confirmation before communication of part 2 of the data. Instead both parts of the data must be provided to the data subject as it follows from the request made.
情況 2：若當事人選擇資料之第 1 部分及第 2 部分之按鈕，控管者不得僅提供資料之第 1 部分，亦不得於提供資料之第 2 部分前要求提出新的請求。實則，控管者必須將這兩部分資料都提供予當事人，因為當事人所提出之請求包含這兩部分資料。

145. The use of a layered approach will not be considered appropriate for all controllers or in all situations. It should only be used when it would be difficult for the data subject to comprehend the information if given in its entirety. In other words, the

controller needs to be able to demonstrate that the use of layered approach adds value for the data subject in helping them understand the information provided. A layered approach would therefore only be considered appropriate when a controller processes a vast amount of personal data about the data subject making a request and where there would be apparent difficulties for the data subject to grasp or comprehend the information if it were to be provided all at once. The fact that it would require great effort and resources from the controller to provide the information under Art. 15 is not in itself an argument for using a layered approach.
分層方法之使用不會被認為適合所有控管者或所有情況。只有在當事人難以理解資訊之全部內容時，才應使用此等方法。換言之，控管者需要證明使用分層方法得為當事人增加價值，協助其理解所提供之資訊。因此，只有在控管者運用大量關於提出請求之當事人的個人資料，且若一次提供所有資訊顯然會使當事人難以掌握或理解該等資訊時，分層方法才會被認為屬適當。控管者需要付出大量努力及資源來提供第 15 條所定資訊，此事實本身並不能成為使用分層方法的理由。

5.2.5 Format
格式

146. According to Art. 12(1), information under Art.15 shall be provided in writing, or by other means, including, where appropriate, by electronic means. As regards access to the personal data undergoing processing, Art. 15(3) states that where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The GDPR does not specify what a commonly used electronic form is. Thus there are several conceivable formats that can be used. What is considered to be a commonly used electronic form will also vary over time.
依據第 12 條第 1 項，第 15 條所定資訊應以書面形式或其他方式提供，包括於適當時以電子形式提供。至於近用正在運用之個人資料，第 15 條第 3 項規定，若當事人以電子形式提出要求，除非當事人另有說明，應以常用電子形式提供該資訊。因 GDPR 並未說明什麼是常用電子形式，因此可使用幾種現有常見格式。常用電子形式的範圍也會隨著時間而有所變化。

147. What could be considered as a commonly used electronic form should be based upon the reasonable expectations of the data subjects and not upon what format the controller uses in its daily operations. The data subject should not be obliged to buy specific software in order to get access to the information.
常用電子形式的範圍應以當事人之合理期望為基礎，而非基於控管者於其日常運作中使用之格式。不應要求當事人購買特定軟體來取得資訊近用。

148. When deciding upon the format in which the copy of the personal data and the information under Art. 15 should be provided, the controller needs to keep in mind that the format must enable the information to be presented in a way that is both intelligible and easily accessible. It is important that the data subject is provided with information in an embodied, permanent form (text, electronic). Since the information should persist over time, information in writing, including by electronic means, is in principle preferable over other forms. The copy of the personal data could, when appropriate, be stored on an electronic storage device, such as CD or USB.
在決定提供個人資料之複製本及第 15 條所定資訊之格式時，控管者應確保該格式必須使資訊以可理解及易近用之方式呈現。重要的是，當事人取得的資訊應以一種可體現資訊且永久的形式（紙本、電子）呈現。因資訊應該隨著時間推移而持續存在，原則上書面資訊（包括電子形式）比其他形式更為恰當。個人資料之複製本得儲存於電子儲存裝置上，如光碟或隨身碟中（於適當情形下）。

149. It should be noted that for a controller to be able to consider that data subjects have been provided with a copy of personal data it is not enough to have provided them with access to their personal data. For the requirement to provide a copy of personal data to be fulfilled and in case the data are provided electronically/digitally, the data subjects need to be able to download their data in a commonly used electronic form.
應注意者為，為使控管者能夠被認為已向當事人提供個人資料之複製本，僅向其提供其個人資料之近用並不足夠。為滿足提供個人資料複製本之請求，若資料係以電子/數位方式提供，當事人需要能夠以常用電子形式下載其資料。

150. It is the responsibility of the controller to decide upon the appropriate form in which the personal data will be provided. The controller can, although is not necessarily obliged to, provide the documents which contain personal data about the data subjects making the request, as such and in their original form. The controller can for example, on a case-by-case basis, provide access to a copy of medium given the need for transparency (for example, to verify the accuracy of the data held by the controller in the event of a request for access to the medical file or an audio recording whose transcript is disputed). However, the CJEU, in its interpretation of the right of access under the Directive 95/46/EC, stated that "for *[the right of access]* to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant,

exercise the rights conferred on him"[76]. Unlike the directive, the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing. Hence, there is no contradiction between the wording of the GDPR and the ruling by the CJEU regarding this matter. The word summary in the ruling should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access, but is merely a way to present all that data without giving systematically access to the actual documents. Since the compilation needs to contain a copy of the personal data, it should be stressed that it cannot be made in a way that somehow alters or changes the content of the information.

控管者有責任決定以何種適當形式提供個人資料。控管者得（但不一定有義務）提供包含當事人個人資料之文件並以其原始形式提供。例如，有鑑於透明化要求，控管者視個案情況提供媒介複製本之近用（例如，於請求近用醫療檔案或錄音檔案有爭議的情況下，為查驗控管者持有資料之正確性）。然而，歐盟法院於依據第 95/46/EC 號指令對近用權所作之解釋中指出，「為遵守*[近用權]*，僅需以可理解之形式向申請人提供該等資料之完整摘要，亦即，一種允許其理解該等資料並確認資料是否正確及依據該指令運用之形式，使其得於相關情況下行使其所享權利」[76]。與該指令不同者為，GDPR 明示規定向當事人提供正在運用個人資料之複製本的義務。然而，這並不代表當事人永遠有權取得包含個人資料之文件複製本，而是有權取得該等文件中正在被運用之個人資料的未經變更複製本。此等個人資料之複製本得透過包含近用權所涉及所有個人資料之彙編本提供，但前提為該彙編本能夠讓當事人理解並確認運用的合法性。因此，GDPR 文字與歐盟法院就此議題所作裁決之間並無衝突。該裁決中「摘要」一詞不應被誤解為彙編中不包含近用權所涵蓋的所有資料，實則，「摘要」僅是一種呈現所有資料但不對實際文件進行全面近用的方式。因該彙編需要包含個人資料之複製本，應強調者為，其不能以替換或變更資訊內容的方式備置。

Example: A data subject has been insured with an insurance company for many years. Several insured incidents have occurred. In each case there has been some

[76] CJEU, Joined Cases C-141/12 and 372/12, YS and Others, para. 60.
歐盟法院，合併案件 C-141/12 及 372/12，YS 及他人，第 60 段。

written correspondence through e-mail between the data subject and the insurance company. As the data subject had to provide information on the specific circumstances of each incident the correspondence entails a lot of personal information about the data subject (hobbies, flatmates, daily habits etc.). In some cases disagreement arose about the insurance company's obligation to compensate the data subject which caused a vast amount of communication back and forth. All this correspondence is stored by the insurance company. The data subject makes an access request. In this situation the controller does not necessarily have to provide the e-mails in their original form by forwarding them to the data subject. Instead the controller could choose to compile the e-mail correspondence containing the data subject's personal data in a file that is provided to the data subject.

範例：當事人已於一家保險公司投保多年，並發生過幾次保險事故。於各事故中，當事人及保險公司之間均有透過電子郵件進行書面通訊。因當事人必須提供各事故之具體情況，通訊中包含很多關於當事人之個人資料（嗜好、室友、日常習慣等）。於特定情況下，雙方對保險公司賠償當事人之義務產生意見分歧，導致大量來回溝通。所有該等信件均係由保險公司保存。當事人提出近用請求。於此情況下，控管者不一定要將該等電子郵件以原始形式轉發給當事人。實則，控管者得選擇將包含當事人個人資料之電子郵件信件進行彙編後提供予當事人。

151. Making some kind of compilation and extraction of the data that makes the information easy to comprehend is also a way of complying with the requirements to provide the information in a way that is both intelligible and easily accessible.
對資料進行某種彙編及擷取，使資訊易於理解，也是符合以可理解及易近用方式提供資訊之規範的一種方式。

152. In this context, it is important to remember that there is a distinction between the right to obtain access under Art. 15 GDPR and the right to receive a copy of administrative documents regulated in national law, the latter being a right to always receive a copy of the actual document. This does not mean that the right of access under Art. 15 GDPR excludes the possibility to receive a copy of the document/media on which the personal data appear.
於此情況下，應注意者為，GDPR 第 15 條所定取得近用權與國家法律規定取得行政文件複製本之權利間有所區別，後者為永遠可取得實際文件複製本之權利。這並不代表 GDPR 第 15 條所定近用權排除取得個人資料之文件/媒介複製本之可能性。

153. In some cases, the personal data itself sets the requirements in what format the

personal data should be provided. When the personal data for example constitutes handwritten information by the data subject, the data subject needs in some cases to be provided with a photocopy of that handwritten information since the handwriting itself is personal data. That could especially be the case when the handwriting is something that matters to the processing, e.g. scripture analysis. The same applies in general for audio recordings since the voice of the data subject itself is personal data. In some cases, however, access can be given by providing a transcription of the conversation, e.g. if agreed upon between the data subject and the controller.

於特定情況下，個人資料本身會限制其應以何種格式提供。例如，當事人之個人資料若為其手寫資訊時，控管者於特定情況下需要向當事人提供手寫資訊之影本，因為筆跡本身就是個人資料，特別是當筆跡是對運用而言具有意義的情況下，例如筆跡分析。一般而言，這也適用錄音，因為當事人聲音本身就是個人資料。然而，於特定情況下，得透過提供對話的逐字稿提供近用，例如當事人及控管者達成合意時。

154. It should be noted that the provisions on format requirements are different regarding the right of access and the right of data portability. Whilst the right of data portability under Art. 20 GDPR requires that the information is provided in a machine readable format, the right to information under Art. 15 does not. Hence, formats that are considered not to be appropriate when complying with a data portability request, for example pdf-files, could still be suitable when complying with a request of access.

應注意者為，關於近用權及資料可攜權之格式要求有不同規範。GDPR 第 20 條所定資料可攜權要求以機器可讀之格式提供資料，而第 15 條所定資訊權則無此規範。因此，於回覆資料可攜權請求時被認為不適當的格式（例如 PDF 檔案），於回覆近用請求時仍可使用。

5.3 Timing for the provision of access
提供近用的時間點

155. Art. 12(3) requires that the controller provides information on action taken on a request under Art. 15 to the data subject without undue delay and in any event within one month of receipt of the request. This deadline can be extended by a maximum of two months taking into account the complexity and the number of the requests, provided that the data subject has been informed about the reasons for such delay within one month of the receipt of the request. This obligation to inform the data subject on the extension and its reasons should not be confused with the information that has to be given without delay and at the latest within one month when the controller does not take action on the request, as follows by Art.

12(4).
第 12 條第 3 項規定，控管者應依據第 15 條規範向當事人提供其所採取行動之相關資訊，不得無故拖延，且無論如何應於收到請求後一個月內提供。考量到請求之複雜性及數量，此期限最多得延長兩個月，但前提為應於收到請求後一個月內向當事人告知此延期之原因。此等通知當事人延期及其原因之義務，不應與第 12 條第 4 項所定於控管者不就請求採取行動的情況下必須至遲於一個月內提供資訊、不得無故拖延的義務混淆。

156. The controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which in other words means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so. The EDPB also considers that the timing to answer the request in some situations must be adapted to the storage period in order to be able to provide access[77].
控管者原則上就請求作出回覆並提供第 15 條所定資訊，不得無故拖延；換言之，控管者應盡快提供資訊。亦即，若有可能於比一個月更短的時間內提供必要資訊，控管者就應該這樣做。EDPB 亦認為，於特定情況下，為能夠提供近用 [77]，回覆請求之時間必須依據保存期間進行調整。

157. The time limit starts when the controller has received an Art. 15 request, meaning when the request reaches the controller through one of its official channels. It is not necessary that the controller in fact has taken notice of it. However, when the controller needs to communicate with the data subject due to the uncertainty regarding the identity of the person making the request there may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay. The same applies for when a controller has asked, in accordance with Recital 63, a data subject to specify the processing operations to which the request relates.
時限自控管者收到第 15 條請求時（即請求透過其官方管道傳送予控管者時）起算，不管控管者事實上是否已注意到該請求。然而，當控管者因不確定提出請求之人的身分而需要與當事人溝通時，得暫停該時間之計算，直到控管者自當事人處取得必要資訊為止，但前提為控管者已要求提供額外資訊，不得無故拖延。此亦適用控管者依據前言第 63 點要求當事人明確說明請求所涉運用作業的情況。

[77] See 2.3.3.
見 2.3.3 節。

Example: Following the reception of the request, a controller reacts immediately and asks the information it needs to confirm the identity of the person making the request. The latter replies only several days later and the information that the data subject sends to verify the identity does not seem sufficient which requires the controller to ask for clarifications. In this situation there will be a suspension in time until the controller has obtained enough information to verify the identity of the data subject.
範例：在收到請求後，控管者立即做出回覆，並要求提供必要資訊以確認提出請求之人之身分。後者在幾日後才回覆，而當事人為確認身分而提供之資訊似乎並不充分，控管者因此必須請當事人再度說明。於此情況下，回覆時限之計算將會暫停，直到控管者取得充分資訊可確認當事人身分為止。

158. The time period needs to be calculated in accordance with Regulation No 1182/71[78].
此等時限應依據第 1182/71 號規則進行計算[78]。

Example 1: An organisation receives a request on 5 March. The time limit starts from the same day. This gives the organisation until and including 5 April to comply with the request, at the latest.
範例 1：組織於 3 月 5 日收到請求。時限自當日起算。該組織因此至遲應於 4 月 5 日（含）前遵守該請求。

Example 2: If the organisation receives a request on 31 August, and as the following month is shorter there is no corresponding date, the date for response, at the latest, is the last day of the following month, hence 30 September.
範例 2：若組織於 8 月 31 日收到請求，因次月較短因此無相應日期，則最晚回覆日期為次月最後一日，即 9 月 30 日。

159. If the last day of this time period falls on a weekend or a public holiday, the controller has until the next working day to respond.
若時限之最後一日為週末或國定假日，控管者應於次一營業日前作出回應。

160. Under certain circumstances the controller can extend the time to respond on a request of access by two further months if necessary, taking into account the

[78] Regulation (EEC, EURATOM) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits.
1971 年 6 月 3 日歐盟理事會關於判斷適用期限、日期及時限第 1182/71 號規則（EEC，EURATOM）。

complexity and number of the requests. It should be emphasised that this possibility is an exemption from the general rule and should not be overused. If controllers often find themselves forced to extend the time limit, it could be an indication of a need to further develop their general procedures to handle requests.
於特定情況下，如有必要，考量到請求之複雜性及數量，控管者得將對近用請求之回覆時間再延長兩個月。應強調者為，此可能性是對通用規定之一種豁免，不應該被過度使用。若控管者經常發現自己被迫需延長時限，這可能表示其需要進一步調整其處理請求的通用程序。

161. What constitutes a complex request varies depending upon the specific circumstances of each case. Some of the factors that could be considered relevant are for example:
構成複雜請求的要件會依據各案件的具體情況而有所不同。例如，被認為相關之因素包括：

- the amount of data processed by the controller,
控管者運用之資料量；

- how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation,
資訊之保存方式，特別是在難以檢索資訊的情況下，例如資料由組織之不同單位運用時；

- the need to redact information when an exemption applies, for example information regarding other data subjects, and
當適用豁免時，需要遮蔽資訊之情況，例如關於其他當事人之資訊；及

- when the information requires further work in order to be intelligible.
當資訊需要進一步處理以使其可被理解時。

162. The mere fact that complying with the request would require a great effort does not make a request complex. Neither does the fact that a big company receives a large number of requests automatically trigger an extension of the time limit. However, when a controller temporarily receives a large amount of requests, for example due to an extraordinary publicity regarding their activities, this could be regarded as a legitimate reason for prolonging the time of the response. Nevertheless, a controller, especially one who handles a large amount of data, should have routines and mechanisms in place in order to be able to handle requests within the time limit under normal circumstances.

僅因遵守請求需要付出巨大努力之事實，並不能使請求被認定為複雜。大公司收到大量請求之事實也不會自動觸發時限之延展。然而，當控管者暫時收到大量之請求時，例如因其相關業務之特別宣傳活動，則可能被視為延長回覆時間的正當理由。然而，控管者，尤其是運用大量資料之控管者，應該備有相關流程與機制，俾以能夠於正常情況下於時限內處理請求。

6 LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS
近用權之限縮及限制

6.1 General remarks
一般性評論

163. The right of access is subject to the limits that result from Art. 15(4) GDPR (rights and freedoms of others) and Art. 12 (5) GDPR (manifestly unfounded or excessive requests). Furthermore, Union or Member State law may restrict the right of access in accordance with Art. 23 GDPR. Derogations regarding the processing of personal data for scientific, historical research or statistical purposes or archiving purposes in the public interest can be based on Art. 89(2) and Art. 89(3) GDPR accordingly and for processing carried out for journalistic purposes or the purpose of academic artistic or literary expression on Art. 85(2) GDPR.
近用權受 GDPR 第 15 條第 4 項（他人之權利及自由）及 GDPR 第 12 條第 5 項（顯無理由或過度要求）所拘束。此外，歐盟或會員國法律得依據 GDPR 第 23 條限制近用權。為公共利益而就科學、歷史研究或統計目的或建檔目的所為之個人資料運用，可依據 GDPR 第 89 條第 2 項及第 89 條第 3 項限縮近用權，而就新聞目的或學術、藝術或文學表達目的所為之個人資料運用，則可依據 GDPR 第 85 條第 2 項限縮近用權。

164. It is important to note that, apart from the above mentioned limits, derogations and possible restrictions, the GDPR does not allow any further exemptions or derogations to the right of access. That means *inter alia* that the right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subjects request under Art. 15 GDPR[79]. Furthermore, it is not permitted to limit or restrict the right of access in a contract between the controller and the data subject.
應注意者為，除上述之限縮、減損及可能限制之外，GDPR 不允許近用權

[79] Where the controller processes a large quantity of information concerning the data subject, as mentioned in recital 63 GDPR, the controller may request the data subject to specify the information or processing activities to which the request relates. See also section 2.3.1 above.
若控管者處理大量關於當事人之資料，如 GDPR 前言第 63 段所述，控管者得要求當事人說明其請求所涉之資料或運用作業。另見上文第 2.3.1 節。

有任何進一步之豁免或減損。亦即，近用權對於控管者為滿足當事人依據 GDPR 第 15 條提出之要求而必須採取之努力，不存在任何通用性之保留 [79]。此外，亦不允許控管者及當事人透過契約限縮或限制近用權。

165. According to Recital 63, the right of access is granted to data subjects in order to be aware of, and verify, the lawfulness of the processing. The right of access enables, inter alia, the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of personal data[80]. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant[81].
依據前言第 63 段，近用權是授予當事人理解及確認運用合法性之權利。近用權尤其使當事人能夠依據情況請求對其個人資料進行更正、刪除或停用 [80]。然而，當事人無義務說明理由或證明其請求。只要符合 GDPR 第 15 條規範，請求背後之目的並不重要 [81]。

6.2 Article 15 (4) GDPR
GDPR 第 15 條第 4 項

166. According to Art. 15(4) GDPR, the right to obtain a copy shall not adversely affect the rights and freedoms of others. Explanations to this limitation are given in the fifth and sixth sentences of Recital 63. That right 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, the result of those considerations should not be a refusal to provide all information to the data subject. When interpreting Art. 15(4) GDPR special caution has to be taken not to unjustifiably widen the restrictions laid down in Art. 23 GDPR, which are permissible only under strict conditions.
依據 GDPR 第 15 條第 4 項，取得複製本之權利不得對他人之權利及自由產生不利影響。前言第 63 段之第五句及第六句對此限制進行解釋。該權利不應影響他人之權利或自由，包括營業秘密或智慧財產權，特別是保護軟體之著作權。然而，該等考量之結果不應是拒絕向當事人提供所有資訊。於

[80] CJEU, Joined Cases C-141/12 and C-372/12, YS and Others.
歐盟法院，合併案件 C-141/12 及 C-372/12，YS 及他人。

[81] This is without prejudice to any applicable national procedural rules that delineate, for example, the purposes for which information is to be provided to or exchanged between parties to ongoing or prospective (court) proceedings and other ongoing or prospective (legal) claims or causes of action in the context of a legal relationship, provided that – and to the extent that – these national provisions comply with the requirements posed by Art. 23 GDPR.
這並不影響任何適用之國家程序規則，例如，向繫屬中或可能開展之（法院）訴訟程序及其他繫屬中或可能開展之（法律）請求或法律關係中之請求權各方當事人提供或交換資訊之目的，但前提該等國家規定符合 GDPR 第 23 條所定規範。

解釋 GDPR 第 15 條第 4 項時，必須特別注意不應無合理事由擴大 GDPR 第 23 條所定限制，該等限制僅有在嚴格條件下才能實施。

167. Art. 15(4) GDPR applies to the right to obtain a copy of the data, which is the main modality of giving access to the data processed (second provision of Art. 15(1) GDPR). It is also applicable, and rights and freedoms of others shall be taken into account, if access to the personal data is exceptionally granted by other means than a copy. For example, there is no difference justified whether trade secrets are affected by providing a copy or by granting on sight site access to the data subject. Art. 15(4) GDPR is not applicable to the additional information on the processing as stated in Article 15(1) lit. a.-h. GDPR.
GDPR 第 15 條第 4 項適用取得資料複製本之權利，這是對所運用資料提供近用的主要方式（GDPR 第 15 條第 1 項第 2 款規定）。若於特殊情況下，亦可透過複製本以外之其他方式對個人資料進行近用，惟應考量他人之權利及自由。例如，是否會影響他人營業秘密，不應作為選擇提供複製本或現場提供近用予當事人之正當事由。GDPR 第 15 條第 4 項不適用 GDPR 第 15 條第 1 項第 a-h 款所定關於運用之額外資訊。

168. According to Recital 63, conflicting rights and freedoms include trade secrets or intellectual property and in particular the copyright protecting the software. These explicitly mentioned rights and freedoms should be regarded as examples, as in principle any right or freedom based on Union or Member State law may be considered to invoke the limitation of Art. 15(4) GDPR[82]. Thus, the right to the protection of personal data (Art. 8 European Charter of Fundamental Rights) can also be considered as an affected right in terms of Art. 15(4) GDPR). Especially regarding the right to obtain a copy this (the right to data protection of others) is a typical case where the limitation needs to be assessed. Furthermore, the right to confidentiality of correspondence has to be taken into account, for example with regard to private e-Mail-correspondence in the employment context[83]. It is important to note that not every interest amounts to "rights and freedoms" pursuant to Art. 15(4) GDPR. For example, economical interests of a company not to disclose personal data are not to be taken into account when applying Art. 15(4) as long as they are no trade secrets, intellectual property or other protected rights.
依據前言第 63 段，相互衝突的權利及自由包括營業秘密或智慧財產權，特

[82] The weight or priority of the conflicting rights and freedoms is not a question of the definition of the terms "rights and freedoms". However, balancing of such interests is part of a second step of the assessment, whether Article 15 (4) is applicable. See para. 171 below.
相互衝突之權利及自由之權重或優先權並非「權利及自由」用語定義之問題。然而，平衡該等利益是評估之第二步的一部分，即第 15 條第 4 項是否適用。見下文第 171 段。

[83] ECHR, Bărbulescu v. Romania, no 61496/08, para. 80, 5 September 2017.
歐洲人權法院，Bărbulescu 訴羅馬尼亞案，第 61496/08 號，第 80 段，2017 年 9 月 5 日。

別是保護軟體之著作權。該等明確提及之權利及自由應被視為範例，因為原則上任何基於歐盟或會員國法律之權利或自由，均可被視為適用 GDPR 第 15 條第 4 項所定限制[82]。因此，個人資料保護之權利（歐盟基本權利憲章第 8 條）亦可被視為受 GDPR 第 15 條第 4 項影響之權利；特別是關於取得複製本之權利（他人之資料保護權）是需要評估限制之典型案例。此外，亦必須考量到通訊保密之權利，例如於僱傭方面之私人電子郵件通訊[83]。值得注意者為，依據 GDPR 第 15 條第 4 項，並非各項利益均屬「權利及自由」。例如，於適用第 15 條第 4 項時，只要不涉及營業秘密、智慧財產權或其他受保護之權利，公司不揭露個人資料之經濟利益就不會被考慮在內。

169. "Others" means any other person or entity apart from the data subject who is exercising their right of access. Hence, the rights and freedoms of the controller or processor (trade secrets and intellectual property for example) might come into consideration. If the EU legislator had wanted to exclude controllers or processors rights and freedoms, it would have used the term "third party", which is defined in Art. 4(10) GDPR.
「他人」係指除當事人以外之任何其他正在行使其近用權之人或實體。因此，控管者或受託運用者之權利及自由（例如營業秘密及智慧財產權）可能會被考量在內。若歐盟立法者想排除控管者或受託運用者之權利及自由，會使用 GDPR 第 4 條第 10 項定義之「第三人」一詞。

170. The general concern that rights and freedoms of others might be affected by complying with the request for access, is not enough to rely on Art. 15 (4) GDPR. In fact the controller must be able to demonstrate that in the concrete situation rights or freedoms of others would factually be impacted.
關於近用請求可能會影響他人權利及自由之一般考量，僅援引 GDPR 第 15 條第 4 項並不足夠。事實上，控管者必須能夠證明，於具體的情況下，他人之權利或自由會受到實際影響。

> **Example:** A person who is now an adult was cared for by the youth welfare office over a number of years in the past. The corresponding files may possibly contain sensitive information about other persons (parents, social workers, other minors). However, a request for information from the data subject cannot generally be rejected for this reason with reference to Art. 15(4) GDPR. Rather, the rights and freedoms of others must be examined in detail and demonstrated by the youth welfare office as the controller. Depending on the interests in question and their relative weight, providing such specific information may be rejected (e.g. by redacting names).
> **範例**：某位成年人過去受到青少年福利辦公室多年的照顧。相關檔案可

能包含他人（父母、社工、其他未成年人）之敏感資訊。然而，依據 GDPR 第 15 條第 4 項，一般不能因為此原因而拒絕當事人之資訊申請。實則，他人之權利及自由必須由青年福利辦公室作為控管者進行詳細之審查及證明。依據相關之利益及其相對權重，提供此等具體資訊之請求可能會被拒絕（例如，透過遮蔽姓名）。

171. With regard to Recital 4 GDPR and the rationale behind Art. 52(1) of the European Charter of Fundamental Rights, the right to protection of personal data is not an absolute right[84]. Hence also the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality. When the Art. 15(4) GDPR assessment proves that complying with the request has adverse (negative) effects on other participants' rights and freedoms (step 1), the interests of all participants need to be weighed taking into account the specific circumstances of the case and in particular the likelihood and severity of the risks present in the communication of the data. The controller should try to reconcile the conflicting rights (step 2), for example through the implementation of appropriate measures mitigating the risk to the rights and freedoms of others**.** As emphasised in Recital 63, protecting the rights and freedoms of others by virtue of Art. 15(4) GDPR should not result in a refusal to provide all information to the data subject. This means, for example, where the limitation applies, that information concerning others has to be rendered illegible as far as possible instead of rejecting to provide a copy of the personal data. However, if it is impossible to find a solution of reconciliation, the controller has to decide in a next step which of the conflicting rights and freedoms prevails (step 3).

就 GDPR 前言第 4 段及歐盟基本權利憲章第 52 條第 1 項背後理由而言，保護個人資料之權利並非一項絕對權利 [84]。因此，近用權之行使亦必須依據比例原則與其他基本權利達成平衡。當 GDPR 第 15 條第 4 項之評估證明，遵守請求對其他參與者之權利及自由有不利（負面）影響時（第 1 步），需要權衡所有參與者之利益，並考量到案件之具體情況，特別是資料交流中存在風險之可能性及重大性。控管者應努力調和相互衝突之權利（第 2 步），例如透過實施適當措施以緩解對他人權利及自由之風險。如前言第 63 段所強調，依據 GDPR 第 15 條第 4 項保護他人之權利及自由不應導致拒絕向當事人提供所有資訊。亦即，如於適用限制的情況下，應盡可能遮蔽他人資訊，而非拒絕提供個人資料之複製本。然而，若不可能找到調和的

[84] See, for example, also CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010, para. 48.
範例另見歐盟法院，合併案件 C-92/09 及 C-93/09，Volker und Markus Schecke GbR 及 Hartmut Eifert 訴 Land Hessen [GC]案，2010 年 11 月 9 日，第 48 段。

解決方案，控管者於下一步則需決定以哪項衝突權利及自由優先（第 3 步）。

Example 1: A retailer offers its clients the possibility to order products via a hotline operated by its customer service. For the purpose of proving the commercial transactions, the retailer stores a call recording, in accordance with the strict requirements of applicable legislation. A customer wants to receive a copy of the conversation he had with an agent of the customer service. In a first step, the retailer analyses the request and realises that the record contains personal data that also relate to someone else, namely to the agent of the customer service. In a second step, in order to assess whether providing the copy would affect the rights and freedoms of others, the retailer has to balance the conflicting interests, especially taking into account the likelihood and severity of possible risks to the rights and freedoms of the customer service agent, that are present in the communication of the record to the client. The retailer concludes that there are very limited personal data relating to the customer service agent in the record, only his voice. The retailer/controller finds that the agent is not easily identifiable. Moreover, the content of the discussion is of a professional nature and the data subject was the interlocutor. On the basis of the aforementioned circumstances the controller objectively concludes that the right to access does not adversely affect the rights and freedoms of the agent of the customer service and therefore, the data controller may provide the data subject with the full record, including the parts of the voice record that relate to the agent of the customer service.

範例 1：一家零售商為其客戶提供透過其客服專線訂購產品的選項。為證明商業交易之目的，零售商依據適用法律之嚴格要求保存一份電話錄音。一名客戶擬取得其與客服人員之錄音複製本。零售商第一步就此請求進行分析，發現該對話包含之個人資料亦與他人相關，亦即，與客服人員相關。第二步，為評估提供複製本是否會影響他人之權利及自由，零售商必須平衡相互衝突之利益，特別是考量到客服人員之權利及自由可能面臨風險之可能性及重大性，該等風險存在於向客戶提供錄音的過程中。零售商的結論是，錄音中與客服人員相關的個人資料非常有限，只有該人員的聲音。零售商/控管者發現，該人員不容易被識別。此外，討論的內容屬專業性質，且當事人是對話者。基於上述情況，控管者客觀得出結論，近用權之行使不會對客服人員之權利及自由產生不利影響，因此，資料控管者得向當事人提供完整錄音，包括與客服人員相關之部分。

Example 2: A client of a medical supply store wants access to the measuring results concerning her legs on the basis of Art. 15 GDPR. The medical supply store had measured the data subject's legs in order to craft individual medical compression stockings. Apparently the medical supply store had a lot of experience and had established a special technique to measure accurately. After the measuring in the medical supply store, the client wants to use the measuring results to buy cheaper socks elsewhere (ordering them in an online-shop). The medical supply store partially refuses access to the data on the basis of Art. 15(4) claiming that due to their special, accurate measuring techniques the results were protected as trade secrets. If and in so far the controller is able to prove that:
範例 2：醫療用品商店之客戶擬依據 GDPR 第 15 條對其腿部測量結果進行近用。該醫療用品商店為製作個人醫療壓力襪而測量其腿部數據。該醫療用品商店據稱經驗豐富且備有特殊技術來正確測量。於醫療用品商店測量後，客戶想利用測量結果到其他地方購買更便宜之襪子（於線上商店訂購）。醫療用品商店依據第 15 條第 4 項規定拒絕當事人近用部分資料，主張因其特殊、精確之測量技術，測量結果屬受保護之營業秘密。惟控管者必須證明：

- providing the data subject with information about the measuring results is not possible without revealing how the measurements were taken and
  若不透露測量的執行方式，就無法向當事人提供關於測量結果之資訊；及

- the information about how the measurements were taken including, if relevant, the exact determination of the measuring points are trade secrets
  執行測量方式之資訊（包括相關測量點之確切位置）屬營業秘密；

they may apply Art. 15(4).
始得適用第 15 條第 4 項。

The controller would still have to provide any possible information about the measuring results that would not reveal its trade secret, even if that would imply the effort to revise and edit the results.
控管者仍然必須提供任何不會揭露其營業秘密之測量結果資訊，即使控管者因此需耗費心力變更及編輯測量結果。

Example 3: GAMER X is registered as a user on the gaming platform of PLATFORM Y. One day, GAMER X is notified that his online account has been restricted. As he is unable to log in anymore, GAMER X asks the controller for access to all personal data relating to him. In addition, GAMER X requires access to the reasons for the account restriction. PLATFORM Y, the controller of the online gaming platform with which the request has been lodged, informs the users in its general terms and conditions available on its website, that any kind of cheating (mainly by the use of third party software) will entail a periodical or permanent ban from its platform. PLATFORM Y also informs the users in its privacy policy about the processing of personal data for the purpose of detecting gaming cheats, in accordance with the requirements set out in Art. 13 GDPR.

範例 3：玩家 X 於遊戲平台 Y 上登記為使用者。有一天，玩家 X 被通知其線上帳戶遭限制。因其無法再登入帳戶，玩家 X 向控管者提出請求近用與其相關之所有個人資料。此外，玩家 X 亦請求近用帳戶限制之原因。收到該請求之控管者為線上遊戲平台 Y，於其網站上提供之一般條款及條件中告知使用者，任何形式之作弊行為（主要是透過使用第三方軟體）均將導致暫時或永久禁止進入該平台。平台 Y 亦於其隱私權政策中告知使用者，依據 GDPR 第 13 條所定要求，其為偵測遊戲作弊行為而運用個人資料。

Upon receipt of GAMER X's request for access, PLATFORM Y should provide GAMER X with a copy of the personal data processed about GAMER X. Regarding the reason for the account restriction, PLATFORM Y should confirm GAMER X that it decided to restrict GAMER X's access to online games due to the use of one or repeated gaming cheats which are in violation with the general terms of use. In addition to the information provided about the processing for the purpose of gaming cheat detection, PLATFORM Y should grant GAMER X access to the information it has stored about GAMER X's gaming cheats which led to the restriction. In particular, PLATFORM Y should provide GAMER X with the information that led to the restriction of the account (e.g. log overview, date and time of cheating, detection of third party software,…) in order for the data subject to verify that the data processing has been accurate.

在收到玩家 X 之近用請求後，平台 Y 應向玩家 X 提供一份其運用玩家 X 個人資料之複製本。關於帳戶限制之原因，平台 Y 應向玩家 X 確認，因為玩家 X 使用一項或多項違反一般使用條款之遊戲作弊行為，平台 Y 決定限制玩家 X 使用其帳戶。除提供其為偵測遊戲作弊行為而進行運用之

資訊外，平台 Y 應允許玩家 X 近用其所保存關於玩家 X 遊戲作弊行為且導致帳戶遭限制之資訊。具體而言，平台 Y 應該向玩家 X 提供導致其帳戶遭限制之資訊（例如，日誌概覽，作弊之日期與時間，第三方軟體之檢測等），俾以當事人確認資料運用是否正確。

However, according to Art. 15(4) and Recital 63 GDPR, PLATFORM Y is not bound to reveal any part of the technical operating of the anti-cheat software even if this information is relating to GAMER X as long as this is can be regarded as trade secrets. The necessary balancing of interests under Art. 15(4) will have the result that the trade secrets of PLATFORM Y preclude the disclosure of this personal data because knowledge of the technical operating of the anti-cheat software could also allow the user to circumvent future cheat or fraud detection[85].
然而，依據第 15 條第 4 項及 GDPR 前言第 63 段，平台 Y 無義務揭露反作弊軟體技術作業之任何部分，即使該資訊與玩家 X 有關亦然，只要該等資訊得被視為營業秘密。第 15 條第 4 項所定必要利益平衡之結果為，平台 Y 之營業秘密排除對該等個人資料之揭露，因對反作弊軟體技術操作之瞭解，亦可能讓使用者規避未來作弊或詐欺偵測[85]。

172. If controllers do not provide full access to a data subject under Art. 15(4) GDPR, they have to inform the data subject of the reasons without delay and at the latest within one month (Art. 12 (4) GDPR). The explanatory statement has to refer to the concrete circumstances and allow the data subjects to assess whether they want to take action against the refusal. It must include information about the possibility of lodging a complaint with a supervisory authority (Art. 77 GDPR) and seeking judicial remedy (Art. 79 GDPR).
若控管者未依據 GDPR 第 15 條第 4 項規定向當事人提供完整近用，必須迅即（無論如何應於一個月內）將理由通知當事人，不得無故遲延（GDPR 第 12 條第 4 項）。說明文件必須提到具體情況，並使當事人得以評估其是否要因此採取行動，且其中必須包括關於向監管機關提出申訴（GDPR 第 77 條）及尋求司法救濟（GDPR 第 79 條）之可能性的資訊。

6.3 Article 12(5) GDPR

[85] The extent of the information provided to individuals will be heavily context dependent, taking into account the nature of the data controller and the nature of the breach of the terms of service. In some cases, it may only be possible for the data controller to provide basic information in response to an access request to which Art. 15(4) applies.
考量到資料控管者之性質及違反服務條款之性質，提供個人資料之範圍將於很大程度上取決於案件背景事實。於特定情況下，資料控管者可能僅能提供基本資訊以回覆第 15 條第 4 項適用之近用請求。

GDPR 第 12 條第 5 項

173. Art. 12(5) GDPR enables controllers to override requests for the right of access that are manifestly unfounded or excessive. These concepts have to be interpreted narrowly, as the principles of transparency and cost free data subjects rights must not be undermined.
GDPR 第 12 條第 5 項使控管者能夠拒絕顯無理由或過度之近用權請求。該等概念必須以狹義解釋，因為透明化及無成本之當事人權利原則不能被破壞。

174. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request should be considered on a case by case basis in the context in which it is made in order to decide if it is manifestly unfounded or excessive.
控管者必須能夠向當事人證明，為何控管者認為該請求屬顯無理由或過度，且一旦經要求，應向權責監管機關說明原因。各項請求均應於其提出之背景下逐一個案考量，以判斷其為否顯無理由或過度。

6.3.1 What does manifestly unfounded mean?
顯無理由之意義為何？

175. A request for the right of access is manifestly unfounded, if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach. However, as explained especially in section 3 above, there are only very few prerequisites for requests for the right of access. Therefore, the EDPB emphasises that there is only very limited scope for relying on the « manifestly unfounded » alternative of Art. 12(5) in terms of requests for the right of access.
若採用客觀方法判斷明顯不符合 GDPR 第 15 條規範，則近用權之請求即屬明顯無理由。然而，如上文第 3 節具體說明，提出近用權請求的先決條件非常少。因此，EDPB 強調，就近用權之請求而言，適用第 12 條第 5 項「顯無理由」的情況非常有限。

176. Furthermore, it is important to recall that prior to invoking the restriction, controllers must carefully analyse the content and scope of the request. For example, a request should not be regarded as manifestly unfounded if the request is related to the processing of personal data not subject to the GDPR (in this case, the request should not be dealt with as an Art. 15-request at all).
此外，應注意者為，於援引此限制之前，控管者必須仔細分析請求之內容及範圍。例如，若一項請求與運用不受 GDPR 拘束之個人資料相關，則不

應被視為顯無理由（於此情況下，該請求根本不應被視為第 15 條下之請求）。

177. Other cases in which the applicability of Art. 12(5) is questionable are requests related to information or processing activities that are clearly and obviously not subject to the processing activities of the controller.
第 12 條第 5 項適用性有爭議的其他情況，為涉及資訊或運用作業，且明確、顯然不屬控管者運用作業所拘束之請求。

> **Example**: A data subject addresses a request to a municipal authority concerning data that are processed by a state authority. Instead of arguing that the request is manifestly unfounded it would be more suitable as well as easier for the authority addressed to confirm that these data are not being processed by the authority (first component of Art. 15, the 'whether' personal data are being processed)[86].
> **範例**：當事人向市政主管機關提出關於經國家主管機關運用資料之請求。與其主張該請求顯無理由，不如由該主管機關確認該等資料並未遭該主管機關運用（第 15 條之第一部分，個人資料「是否」被運用）[86]，會更合適也更容易。

178. A controller should not presume that a request is manifestly unfounded because the data subject has previously submitted requests which have been manifestly unfounded or excessive or if it includes unobjective or improper language.
控管者不應因當事人先前提交過顯無理由或過度之請求，或若請求中包含不客觀或不恰當之語言，就推定請求屬顯無理由。

6.3.2 What does excessive mean?
過度之意義為何？

179. There is no definition of the term "excessive" in the GDPR. On the one hand, the wording "in particular because of their repetitive character" in Art. 12(5) GDPR allows for the conclusion that the main scenario for application of this limb with regard to Art. 15 GDPR is linked to the quantity of requests of a data subject for the right of access. On the other hand, the aforementioned phrasing shows that other reasons that might cause excessiveness are not excluded a priori.
GDPR 並未提供「過度」一詞之定義。一方面，依據 GDPR 第 12 條第 5 項中「特別因其重複性」之用語可推論，就 GDPR 第 15 條而言，適用此條款

[86] A different question is whether the authority which the access request was addressed to is entitled to transmit the request to the competent state authority.
另一個議題是，近用權請求所針對之主管機關是否有權將請求轉介予國家主管機關。

之主要情況與當事人提出近用權請求之數量有關。另一方面，上述用語表明，其他可能構成過度的原因並未被預先排除。

180. Certainly, according to Art. 15(3) GDPR regarding the right to obtain a copy, a data subject may submit more than one request to a controller[87]. In the event of requests that could potentially be regarded as excessive, the assessment of "excessiveness" depends on the analysis carried out by the controller and the specifics of the sector in which it operates.
當然，依據 GDPR 第 15 條第 3 項取得複製本之權利，當事人得向控管者提交一項以上之請求 [87]。在有可能被視為過度請求的情況下，對「過度」之評估取決於控管者所進行的分析及其所處產業之具體情況。

181. In case of subsequent requests, it has to be assessed whether the threshold of reasonable intervals (see Recital 63) has been exceeded or not. Controllers must take into account the particular circumstances of the single case carefully.
於後續請求的情況下，必須評估是否已超過合理頻率的門檻（見前言第 63 段）。控管者必須仔細考量個別案件的特殊情況。

182. For example, in the case of social networks, a change in the data set will be expected at shorter intervals than in the case of registers. In the case of business associates, the frequency of contacts among them will be important. Accordingly the "reasonable intervals" within which data subjects may again exercise their right of access are also different. The more often changes occur in the database of the controller, the more often data subjects may be permitted to request access without it being excessive. On the other hand, even a second request by the same data subject might be repetitive under certain circumstances.
舉例而言，於社群網路的情況下，資料集的變更將比登記庫的預期時間間隔更短。於業務夥伴的情況下，雙方接觸頻率則很重要。因此，當事人得再次行使其近用權之「合理間隔」也是不同的。控管者資料庫發生變更的頻率越高，當事人得被允許請求近用的頻率就越高，而不會被認定為過度。另一方面，於特定情況下，即使是同一當事人的第二次請求亦可能會被認為屬重複性質。

183. When deciding whether a reasonable interval has elapsed, controllers should consider, in the light of the reasonable expectations of the data subject:
在判斷合理時間間隔是否已終了時，控管者應依據當事人的合理期望來考

[87] According to Article 15 (3) second sentence, the controller may charge a reasonable fee for further copies requested.
依據第 15 條第 3 款第二句，控管者得對所要求的額外複製本收取合理之費用。

量：

- how often the data is altered – is information unlikely to have changed between requests? If a data pool is obviously not subject to a processing other than storage and the data subject is aware of this, e.g. because of a previous request for the right of access, this might be an indication for an excessive request;
  資料變更之頻率－資訊於兩次請求之間是否不太可能有所變更？若資料池除了儲存外顯然沒有其他運用，而當事人也知道這點，例如因為先前的近用權請求，就有可能是過度請求的跡象；

- the nature of the data – this could include whether it is particularly sensitive;
  資料之性質－這可能包括其是否為特別敏感資料；

- the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed;
  運用之目的－可能包括若揭露運用過程是否可能對請求人造成損害（傷害）；

- whether the subsequent requests concern the same type of information or processing activities or different ones[88].
  後續請求是否涉及同一類型之資訊或運用作業或不同之資訊或運用作業[88]。

Example 1 (carpenter): A data subject lodges access requests every two months with the carpenter that manufactured him or her a table. The carpenter answered the first request completely. When deciding whether a reasonable interval has elapsed, one should consider that the carpenter only occasionally (first bullet point above) and not as part of its core activity processes and collects personal data and it is even less likely that the carpenter often provides services to the same data subject. Indeed, the carpenter did not provide more than one service to the data subject, rendering it unlikely that changes occurred in the dataset concerning the data subject. Notably given the nature and amount of the personal data processed, the risks related to the processing can be considered as low (second bullet point above), such as the purpose of the processing (billing purposes and compliance with obligation to keep records) is not likely to cause

[88] If the subsequent request concerns the same type of information in scope AND time, this is not a question of excessiveness but a question of request for an additional copy, see section 2.2.2.2.
若隨後申請於範圍與時間上涉及相同類型之資訊，這就並非過度之問題，而是要求提供額外複製本之問題，見第 2.2.2.2 條。

detriment to the data subject (third bullet point above). The request furthermore concerns the same information as the last request (forth bullet point above). Such requests may as a consequence be regarded as excessive due to their repetitiveness.

範例 1（木匠）。當事人每兩個月向為其製作桌子的木匠提出近用請求。木匠就第一次請求提供完整回覆。當決定合理時間間隔是否已經終了時，應考量到木匠僅是偶爾（上述第一點）而非於其核心業務活動中運用及蒐集個人資料，更不可能是木匠經常向同一當事人提供服務。事實上，木匠並未向當事人提供超過一次之服務，當事人之資料集因此不可能有所變更。值得注意者為，有鑑於所運用之個人資料性質及數量，與運用相關之風險可被認為屬低度風險（上述第二點），例如，運用之目的（計費目的及遵守保存紀錄之義務）不可能對當事人造成損害（上述第三點）。此外，該請求亦涉及與上次請求相同之資訊（上述第四點）。此請求因其重複性而可能會被視為過度。

Example 2 (social media platform): A social media platform whose core business is the collection and/or processing of personal data of the data subject carries out large-scale complex and continuous processing activities. A data subject that uses the services of the platform lodges access requests every three months. In this case, frequent changes to the personal data relating to the data subject are highly likely (first bullet point above), the broad range of collected data includes inferred sensitive personal (second bullet point above) processed for the purpose of showing relevant content and network members to the data subject (third bullet point). Access requests every three months may –under these circumstances- in principle not be regarded as excessive due to repetitiveness.

範例 2（社群媒體平台）：以蒐集及/或運用當事人個人資料為核心業務之社群媒體平台，進行大規模複雜且持續之運用作業。使用該平台服務之當事人每三個月提交一次近用請求。於此情況下，當事人個人資料之頻繁變更是非常有可能的（上述第一點），廣泛蒐集之資料包括經推論之敏感個人資料（上述第二點），為向當事人顯示相關內容及網路成員之目的而運用（上述第三點）。於此情況下，每三個月一次之近用權請求，原則上不會因為重複性而被視為過度。

Example 3 (credit agencies): Regarding repetitive data subjects' access requests addressed to credit inquiry agencies. The following considerations must be taken into account:
範例 3（信用機關）：關於向信用調查機構重複提出當事人近用請求，必須考量到以下因素：

Similarly to social networks it cannot be ruled out that modifications of the relevant data will occur in the data controller's data stock at much shorter intervals than in other areas (first bullet point above). This results from numerous factors of which the data subject, as a person from outside, is usually not aware due to the complexity of the business model as a whole. The answer to the question as to which types of data were collected for a score value calculation by the controller and which are currently included in the calculation can therefore only be provided by the credit inquiry agency itself. In addition, of special significance is the fact that data processing through credit inquiry agencies and the resulting score value can have far-reaching consequences for the data subject with regard to intended legal transactions, such as the conclusion of purchasing, rent or leasing contracts (third bullet point above).
與社群網路類似，不能排除相關資料之變更會於比其他領域更短之時間內發生於資料控管者之資料庫中（上述第一點）。這是由許多因素所造成，因整個商業模式之複雜性，作為外部人士之當事人一般不瞭解該等因素。因此，關於控管者為計算分數值蒐集哪些類型之資料，及哪些資料目前包括於計算中之問題，僅得由信用調查機構本身提供答案。此外，特別重要的是，透過信用調查機構進行之資料運用及由此產生之分數值，會對當事人於預期法律交易方面產生深遠的影響，如訂定採購、租賃合約等（上述第三點）。

It is not possible to generally determine any specific interval in which the submission of a further access request could be deemed excessive under Art. 12 (5) second sentence GDPR. An overall view of the circumstances of the individual case is rather required. However, given the importance of data processing for the data subjects' reality of everyday life, it can be assumed that a one-year interval between information provided free of charge will in any case be too large for the request to be considered excessive. In the case of credit inquiry agencies, there is only a reason to assume that requests have been submitted excessively if any modification of the data processed by a credit inquiry agency is almost excluded from the requestor's point of view. As a rule, this only applies when several access requests have been groundlessly submitted in a short time. On the other hand, if modifications of the data are possible by

the data subject's participation in economic life, a new request is not excessive.
GDPR 第 12 條第 5 項第二句規定，在任何特定時間間隔屆滿後所提交新近用權請求，並無法就其是否會被視為過度做概括性判斷，這需要對個案情況進行整體檢視。然而，考量到資料運用對當事人現實日常生活之重要性，得假設一年一次免費提供資訊之間隔過大，並不會使此頻率請求被視為過度。就信用調查機構而言，若自請求人之角度來看，除非信用調查機構所運用的資料並無任何變更，才有理由認為請求屬過度。一般情況下，這僅適用於短時間內毫無依據地提交多項近用請求的情況。另一方面，若當事人參與經濟生活之事實可能造成相關資料有所變更，則提出新請求並不會被視為過度。

184. When it is possible to provide the information easily by electronic means or by remote access to a secure system, which means that complying with such requests actually doesn't strain the controller, it is unlikely that subsequent requests can be regarded as excessive.
當有可能透過電子形式或透過遠距近用安全系統輕易提供資訊時，就表示遵守該等請求實際上並不會對控管者造成壓力，則後續請求就不太可能被視為過度。

185. If a request overlaps with a previous request, the overlapping request can generally be regarded as excessive, if and insofar as it covers exactly the same information or processing activities and the previous request is not yet complied with by the controller without reaching the state of "undue delay" (see Art. 12(3) GDPR). In practice, as a consequence both requests could be combined.
若一項請求與先前請求重疊，則只要重疊請求涵蓋完全相同之資訊或運用作業，且控管者尚未回覆之情況尚未構成「無故延遲」，則重疊之請求一般得被認為過度（見 GDPR 第 12 條第 3 項）。在實務上，結果是兩項請求得合併處理。

186. The fact that it would take the controller a vast amount of time and effort to provide the information or the copy to the data subject cannot on its own render a request excessive[89]. A large number of processing activities typically implicates bigger efforts when complying with access requests. However, as stated above, under certain circumstances requests can be regarded as excessive due to other reasons than their repetitive character. In the view of the EDPB this encompasses particularly cases of abusively relying on Art. 15 GDPR, which means cases in which data subjects make an excessive use of the right of access with the only

[89] No proportionality test, see above para. 164.
無比例原則測試，見上文第 164 段。

intent of causing damage or harm to the controller.
控管者需要花費大量時間及精力來向當事人提供資訊或複製本，此事實本身並不能使一項請求被視為過度[89]。於遵守近用權請求時，大量運用作業通常代表更大的努力。然而，如上所述，於特定情況下，請求可能因其他原因（而非因其重複性）而被視為過度。於 EDPB 看來，這特別包括濫用 GDPR 第 15 條的情況，亦即，當事人專為對控管者造成損害或傷害而過度行使近用權的情況。

187. Against this background, a request should not be regarded as excessive on the ground that:
於此背景下，不應以下列理由將一項請求視為過度：

- no reasons are given by the data subject for the request or the controller regards the request as meaningless;
當事人並未就其請求提出原因，或控管者認為此請求沒有意義；

- improper or impolite language is used by the data subject;
當事人使用不恰當或不禮貌的語言；

- the data subject intends to use the data to file further claims against the controller.
當事人擬利用該等資料向控管者提出進一步主張。

188. On the other hand, a request may be found excessive, for example, if:
另一方面，請求於下列情況下可能被認為屬過度：

- an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller or
當事人提出請求的同時表示願意撤回請求以換取控管者提供某種形式之利益；或

- the request is malicious in intent and is being used to harass a controller or its employees with no other purposes than to cause disruption, for example based on the fact that:
該請求為惡意用來騷擾控管者或其員工者，除造成干擾外並無其他目的；例如基於以下事實所提請求：

    - the individual has explicitly stated, in the request itself or in other communications, that it intends to cause disruption and nothing else; or
    當事人於請求本身或其他通訊中明確表示其意圖是造成破壞，

除此之外無其他意圖；或

- the individual systematically sends different requests to a controller as part of a campaign, e.g. once a week, with the intention and the effect of causing disruption[90].
  當事人有系統地向控管者發送不同請求作為某活動之一部分，例如每週一次，其目的及效果是造成干擾[90]。

6.3.3 Consequences
後果

189. In case of a manifestly unfounded or excessive request for the right of access controllers may, according to Art. 12(5) GDPR, either charge a reasonable fee (taking into account the administrative costs of providing information or communication or taking the action requested) or refuse to comply with the request.
於顯無理由或過度請求近用權的情況下，控管者可依據 GDPR 第 12 條第 5 項收取合理之費用（考量到提供資訊或通訊或採取所請求行動之行政成本）或拒絕遵守該請求。

190. The EDPB points out that controllers are - on the one hand - not generally obliged to charge a reasonable fee primary before refusing to act on a request. On the other hand, they aren't completely free to choose between the two alternatives either. In fact, controllers have to make an adequate decision depending on the specific circumstances of the case. Whereas it is hardly imaginable that charging a reasonable fee is a suitable measure in case of manifestly unfounded requests, for excessive requests it is - in line with the principle of transparency - often more appropriate to charge a fee as a compensation for the administrative costs the repetitive requests are causing.
EDPB 指出，控管者一方面通常無義務於拒絕就特定請求採取行動之前收取合理基本費用，另一方面亦並非完全得於這兩種選擇中自由選擇。事實上，控管者必須依據案件之具體情況做出適當決定。雖然很難想像對顯無理由之請求收取合理費用是適當措施，但就過度請求而言，依據透明化原則，收取費用作為處理重複請求之行政成本補償通常較為合適。

191. Controllers must be able to demonstrate the manifestly unfounded or excessive character of a request (Art. 12(5) third sentence GDPR). Hence, it is recommended

[90] "Systematically sending as part of a campaign" means that requests which could easily be combined to one are artificially split into not just a few but many single pieces by the data subject with the apparent intention to cause disruption.
「作為某活動一部分系統性地發送」係指很容易合併成一項之請求被當事人故意分割成許多件（而非僅為幾件）提出，且其目的顯然是為造成干擾。

to ensure a proper documentation of the underlying facts. In line with Art. 12(4), if controllers refuse to act on a request for the right of access in whole or partly, they must inform the data subject without delay and at the latest within one month of receipt of the request of
控管者必須能夠證明請求之顯無理由或過度性質（GDPR 第 12 條第 5 項第三句）。因此，建議就基本事實進行適當記錄。依據第 12 條第 4 項，若控管者拒絕對近用權請求之全部或一部採取行動，其必須迅即（至遲於收到請求後一個月內）將下列資訊通知當事人，不得無故遲延：

- the reason why,
  拒絕之原因；
- the right to lodge a complaint with a supervisory authority,
  向監管機關提出申訴之權利；
- the possibility to seek a judicial remedy.
  尋求司法救濟之可能性。

192. Before charging a reasonable fee based on Art. 12(5) GDPR, controllers should provide an indication of their plan to do so to the data subjects. The latter have to be enabled to decide whether they will withdraw the request to avoid being charged.
於依據 GDPR 第 12 條第 5 項收取合理費用之前，控管者應向當事人說明其有意收取此費用。控管者必須給當事人機會決定是否撤回請求以避免被收費。

193. Unjustified rejections of requests of the right of access can be regarded as infringements of data subject's rights pursuant to Art. 12 to 22 GDPR and can therefore be subject to the exercise of corrective powers by competent supervisory authorities, including administrative fines based on Art. 83 (5) (b) GDPR. If data subjects consider there is an infringement of their data subject rights, they have the right to lodge a complaint based on Art. 77 GDPR.
依據 GDPR 第 12 至 22 條，無合理事由即拒絕遵守近用權請求，可被視為對當事人權利之侵害，因此，得由權責監管機關行使糾正權力，包括依據 GDPR 第 83 條第 5 項第 b 款處以行政罰鍰。若當事人認為其當事人權利受到侵害，有權依據 GDPR 第 77 條提出申訴。

6.4 Possible restrictions in Union or Member States law based on Article 23 GDPR and derogations
基於 GDPR 第 23 條之歐盟或會員國法律之可能限制及減損情況

194. The scope of the obligations and rights provided for in Art. 15 GDPR may be

restricted by way of legislative measures in Union or Member States law. Several Member States have made use of this option[91].
GDPR 第 15 條所定義務及權利之範圍，得透過歐盟或會員國法律之立法措施進行限縮。某些會員國已採行此選項[91]。

195. Controllers, who plan to rely on a restriction based on national law must carefully check the requirements of the provision of the respective national legislation. Furthermore, it is important to note, that restrictions of the right of access in Member States (or Union) law which are based on Art. 23 must strictly fulfil the conditions laid down in this Article. The EDPB has issued the Guidelines 10/2020 on restrictions under Art. 23 GDPR with further explanations on this. In terms of the right of access, the EDPB recalls that controllers should lift the restrictions as soon as the circumstances that justify them no longer apply[92].
擬以國家法規為依據進行限制之控管者，必須仔細檢視相關國家法律規範。此外，應需注意者為，基於第 23 條之會員國（或歐盟）法律中的近用權限制必須嚴格滿足該條所定條件。EDPB 已發布關於 GDPR 第 23 條規定限制之指引 10/2020，就此作進一步解釋。就近用權而言，EDPB 表示，實施限制之合理事由一旦不再適用，控管者應盡快解除限制[92]。

196. Legislative measures laying down the provisions for the application of restrictions under Art. 23 GDPR may also foresee that the exercise of a right is delayed in time, that a right is exercised partially or circumscribed to certain categories of data or that a right can be exercised indirectly through an independent supervisory authority[93].

---

[91] See for example sections 32 to 37 of the German Federal Data Protection Act (BDSG) and Article 5 and 5a of the Polish Act on the Protection of Personal Data.
範例見德國聯邦資料保護法（BDSG）第 32 至 37 條及波蘭個人資料保護法第 5 及 5a 條。

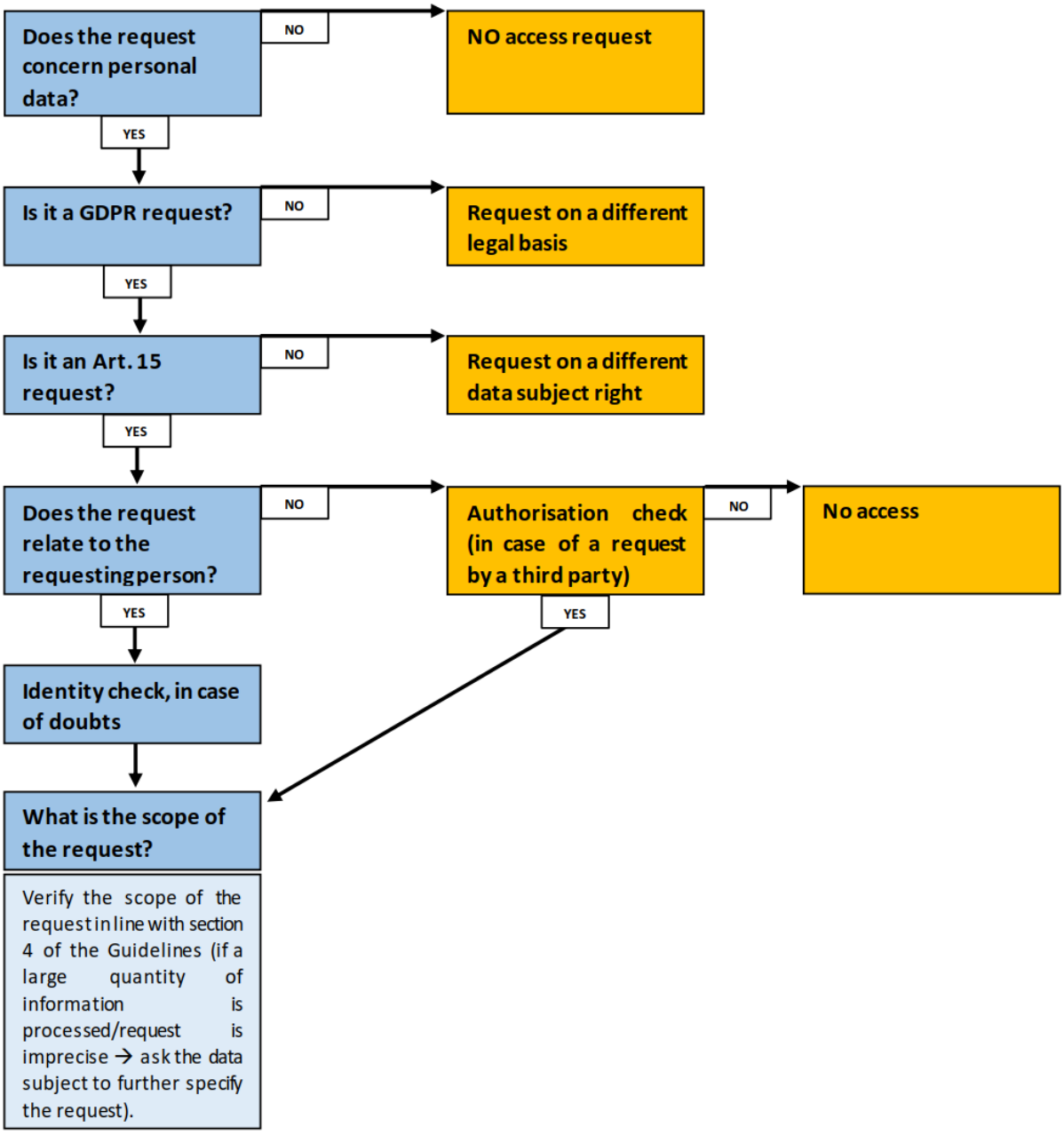
[92] Paragraph 76 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021.
關於 GDPR 第 23 條規定限制之指引 10/2020 第 76 段，第 2.0 版，2021 年 10 月 13 日通過。

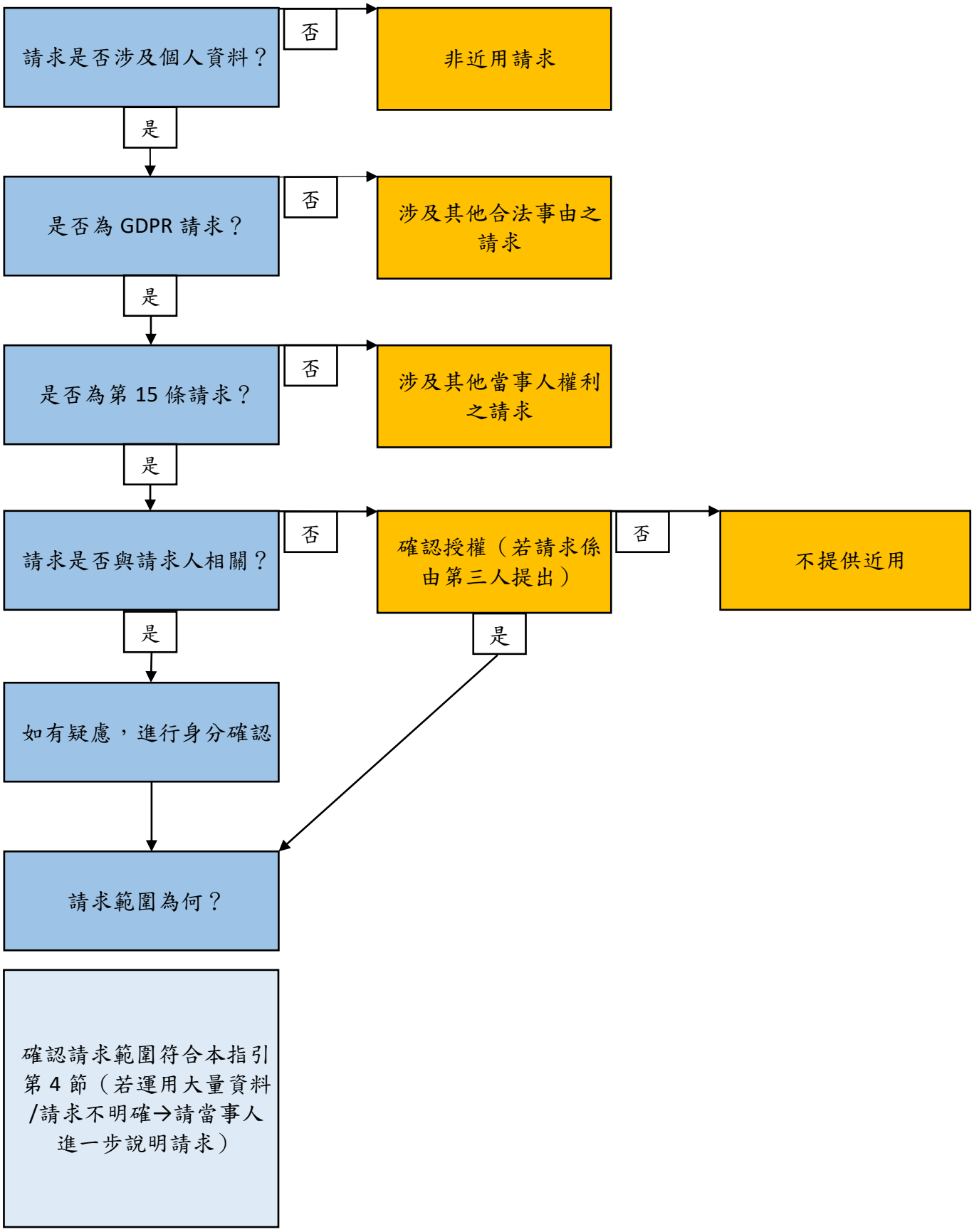
[93] Paragraph 12 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021. Section 34 (3) of the German Federal data protection act for example states that if a public authority doesn´t provide information to a data subject complying with a request for the right of access because of certain restrictions, such information shall be provided to the federal supervisory authority at the request of the data subject, unless the responsible supreme federal authority (of the authority which was subject to the request) determines in the individual case that doing so would endanger the security of the Federation or a Land. The Italian DPCode provides for indirect access (through the authority) in case the access could impact with adverse consequence on a number of interests (e.g. Interest to contrast money laundering) see Art. 2-L of the Italian DPCode.
關於 GDPR 第 23 條所定限制之指引 10/2020 第 12 段，第 2.0 版，2021 年 10 月 13 日通過。舉例而言，德國聯邦資料保護法第 34 條第 3 項規定，若公務機關因特定限制而不向符合近用權請求之當事人提供資訊，則應依據當事人之請求將該等資訊提供予聯邦監管機關，除非負責之聯邦最高主管機關（受理請求之主管機關）就該個案情況判斷提供該等資訊會危及聯邦或州的安全。義大利個人資料保護法規定間接近用（透過主管機關）之情況下，近用可能會造成影響某些利益之不利後果（例如，相較於洗錢防制之利益），見義大利個人資料保護法第 2-L 條。

規定適用 GDPR 第 23 條限制條款之立法措施亦得規範，權利之行使得於時間上進行延展、相關權利亦得就部分或特定類別資料行使，或權利得透過獨立監管機關間接行使[93]。

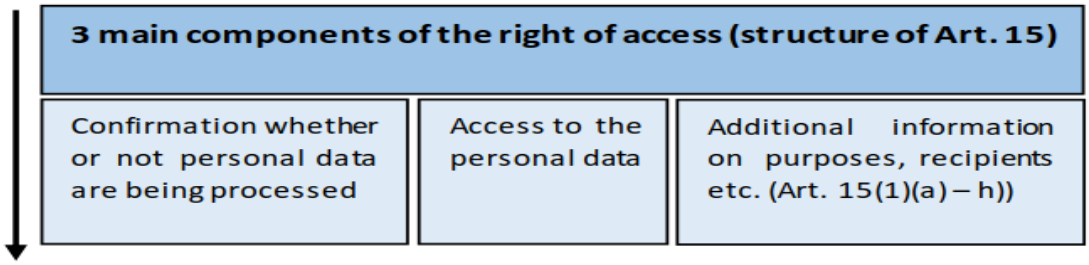
ANNEX – FLOWCHART
附錄－流程圖

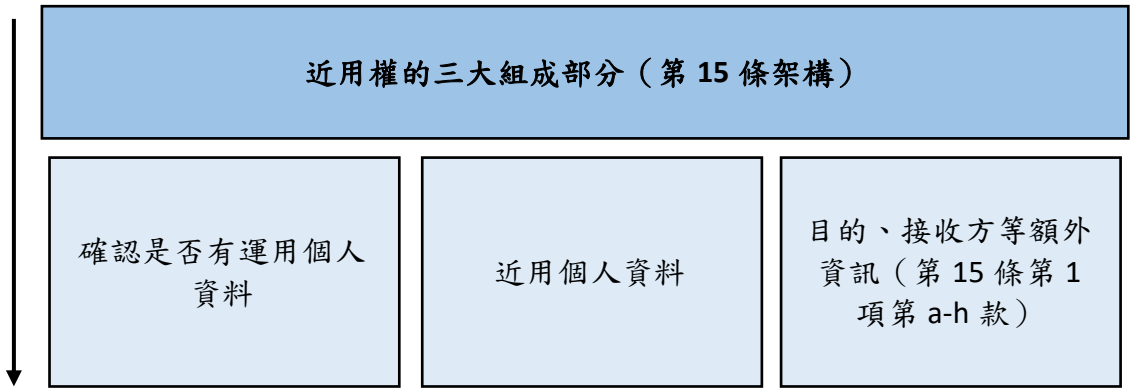
Step 1: How to interpret and assess the request?
第一步：如何解釋及評估請求？



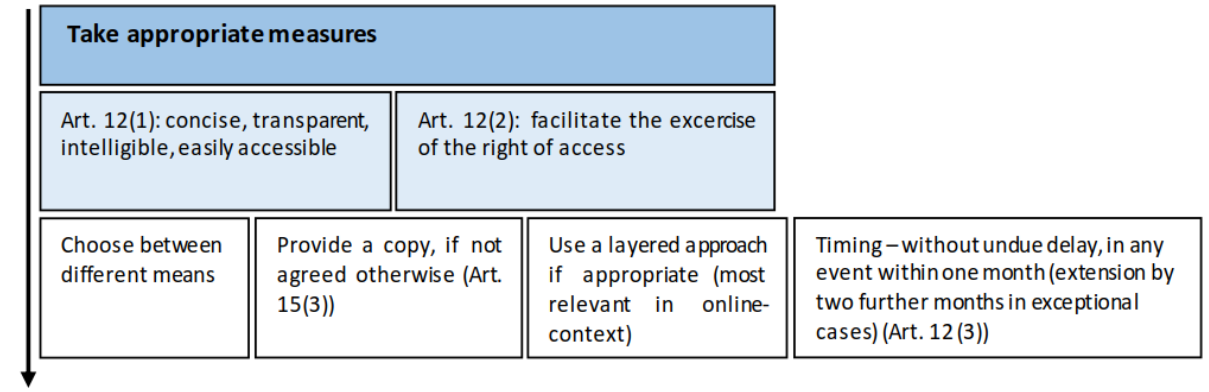

請求是否涉及個人資料？
否
非近用請求
是
是否為 GDPR 請求？
否
涉及其他合法事由之請求
是
是否為第 15 條請求？
否
涉及其他當事人權利之請求
是
請求是否與請求人相關？
否
確認授權（若請求係由第三人提出）
否
不提供近用
是
是
如有疑慮，進行身分確認
請求範圍為何？
確認請求範圍符合本指引第 4 節（若運用大量資料/請求不明確→請當事人進一步說明請求）

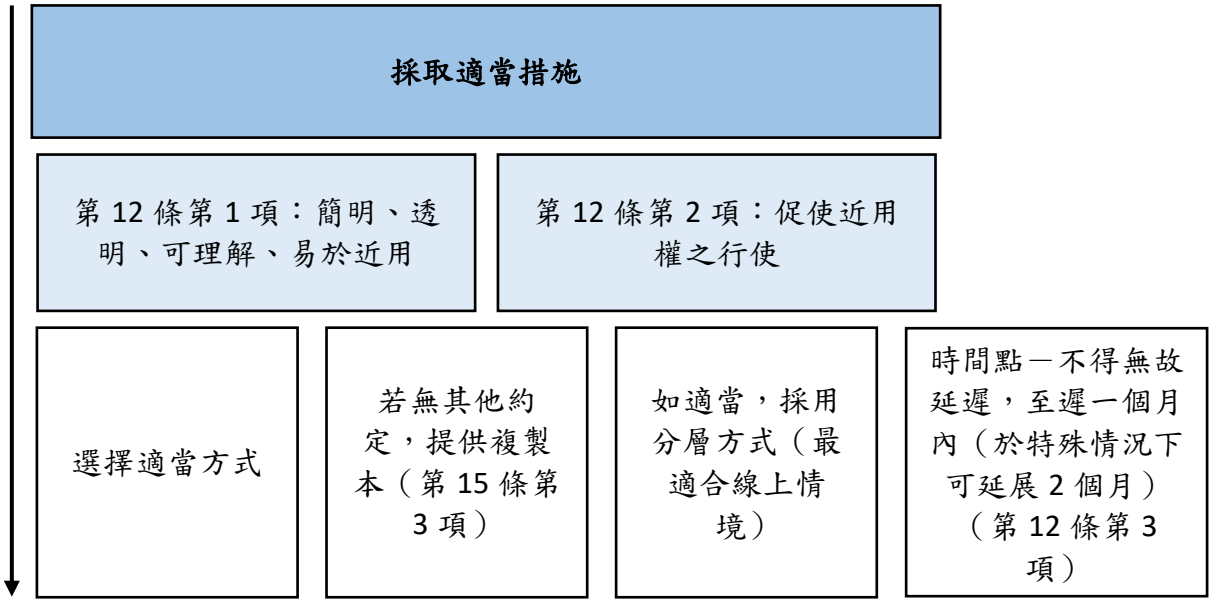
Step 2: How to answer the request (1)?
第二步：如何回覆請求(1)？



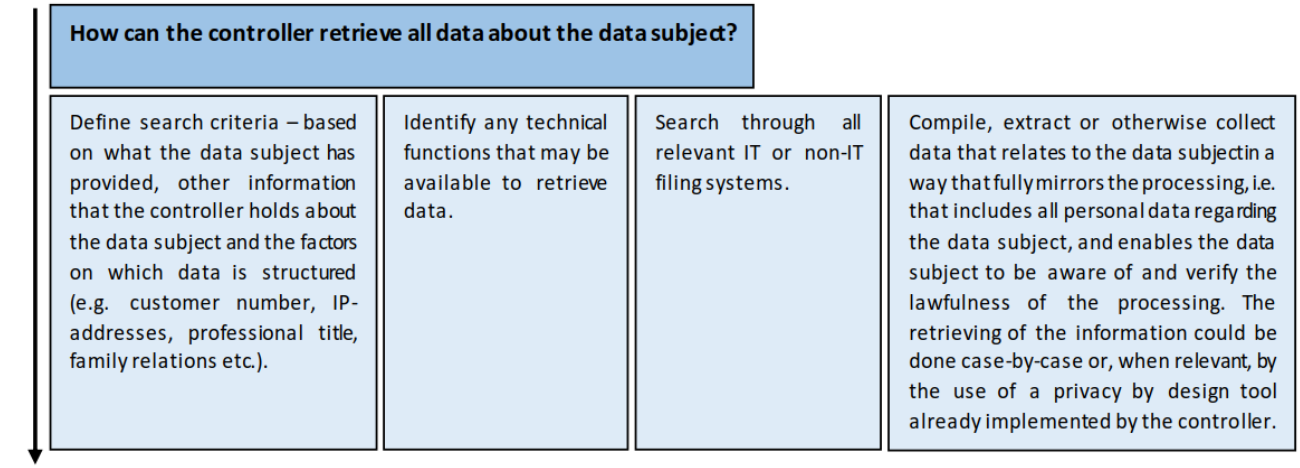


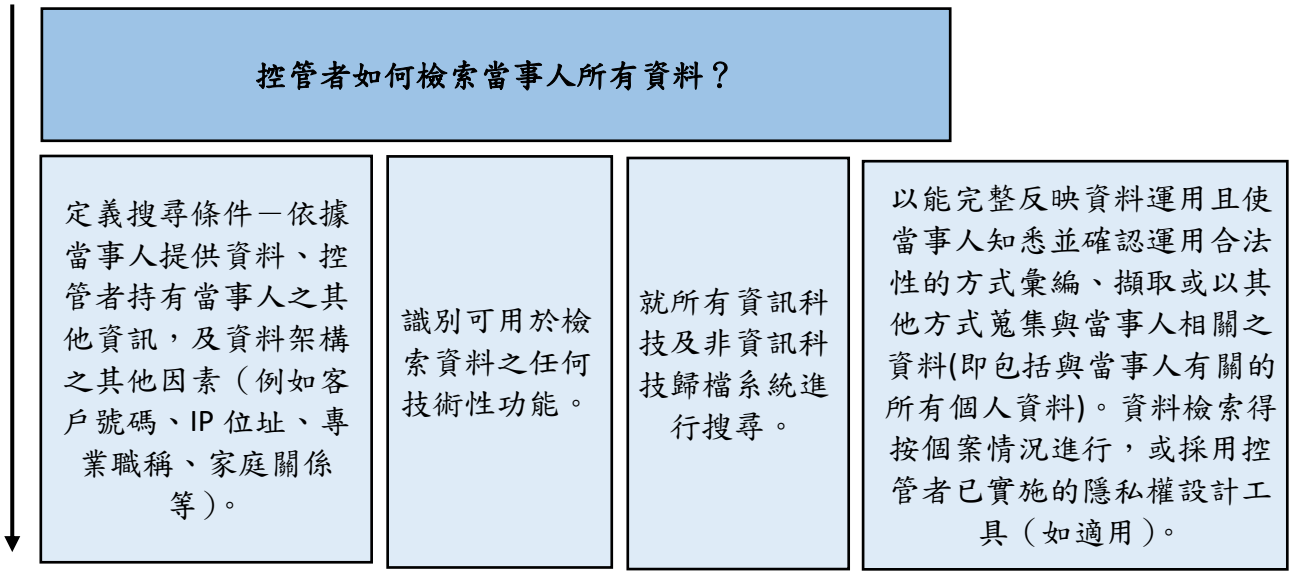
Step 2: How to answer the request (2)?
第二步：如何回覆請求(2)？



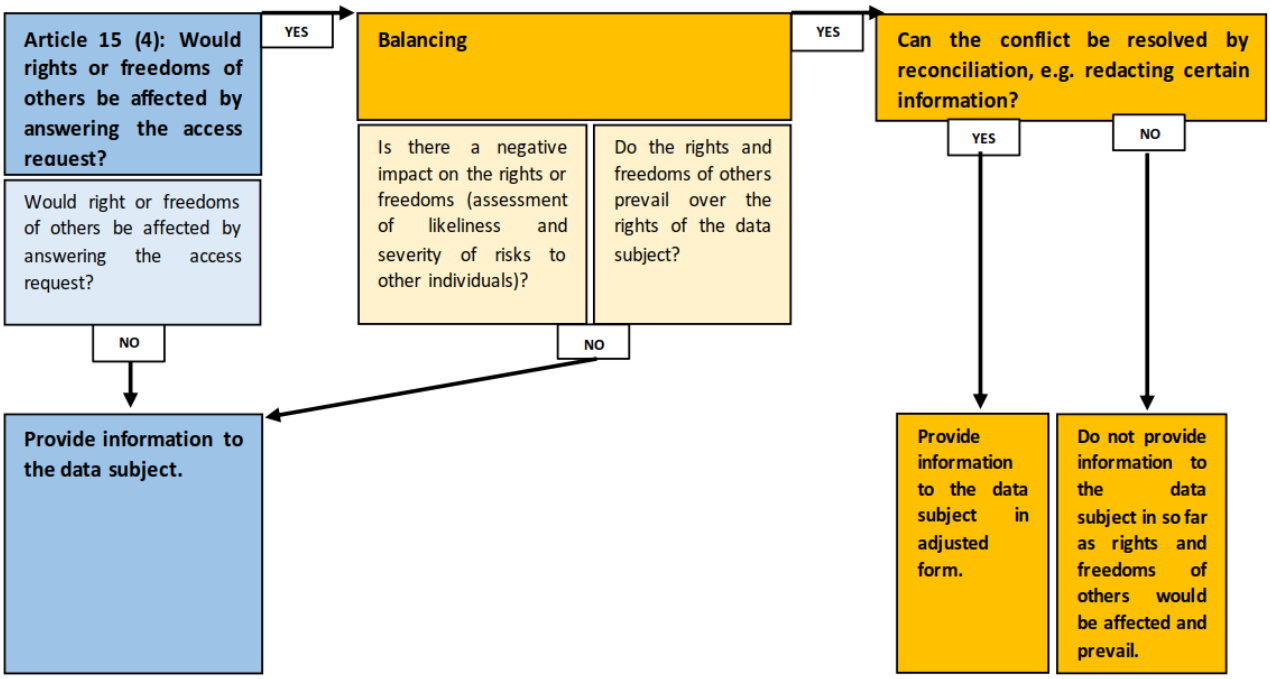


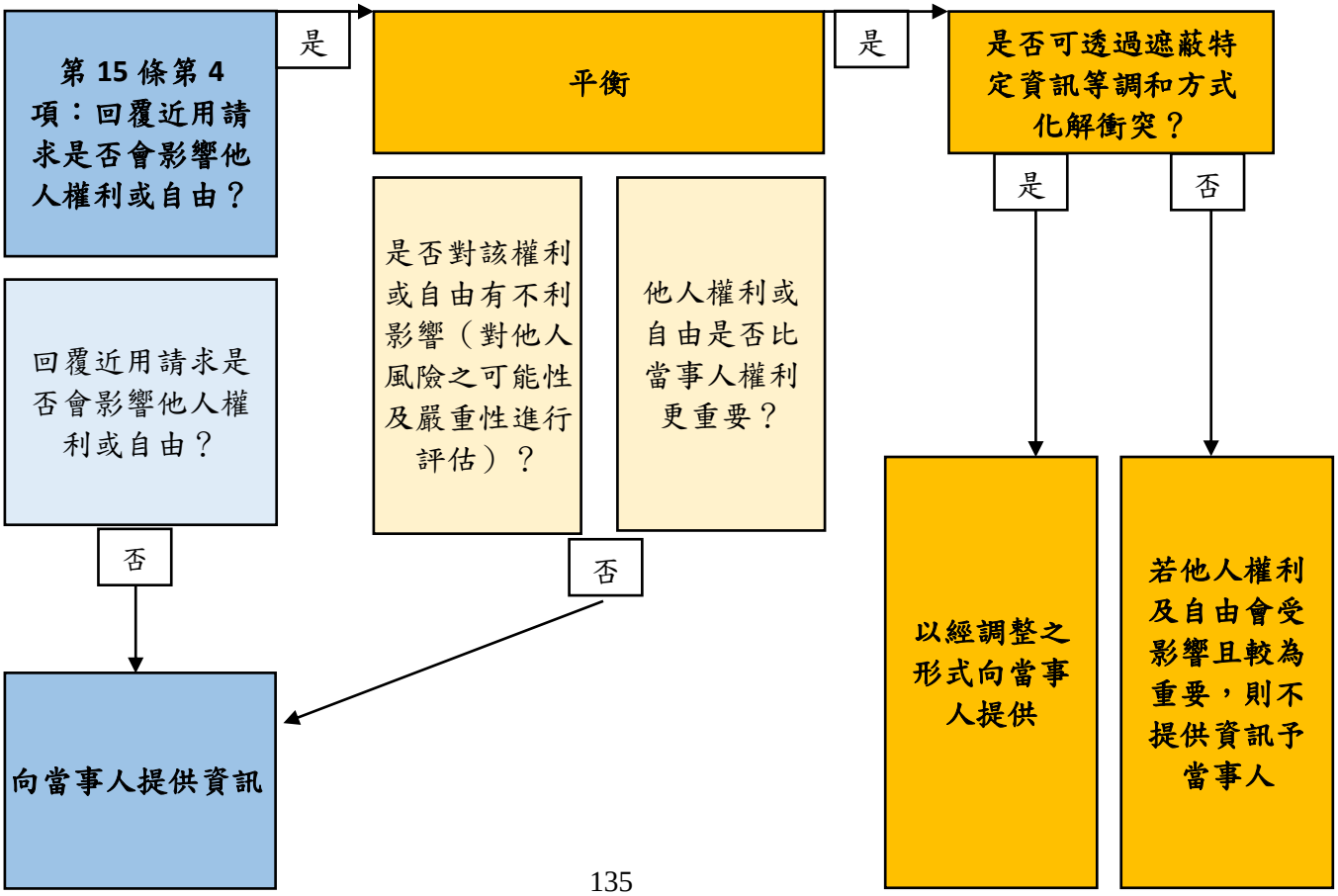
Step 2: How to answer the request (3)?
第二步：如何回覆請求(3)？



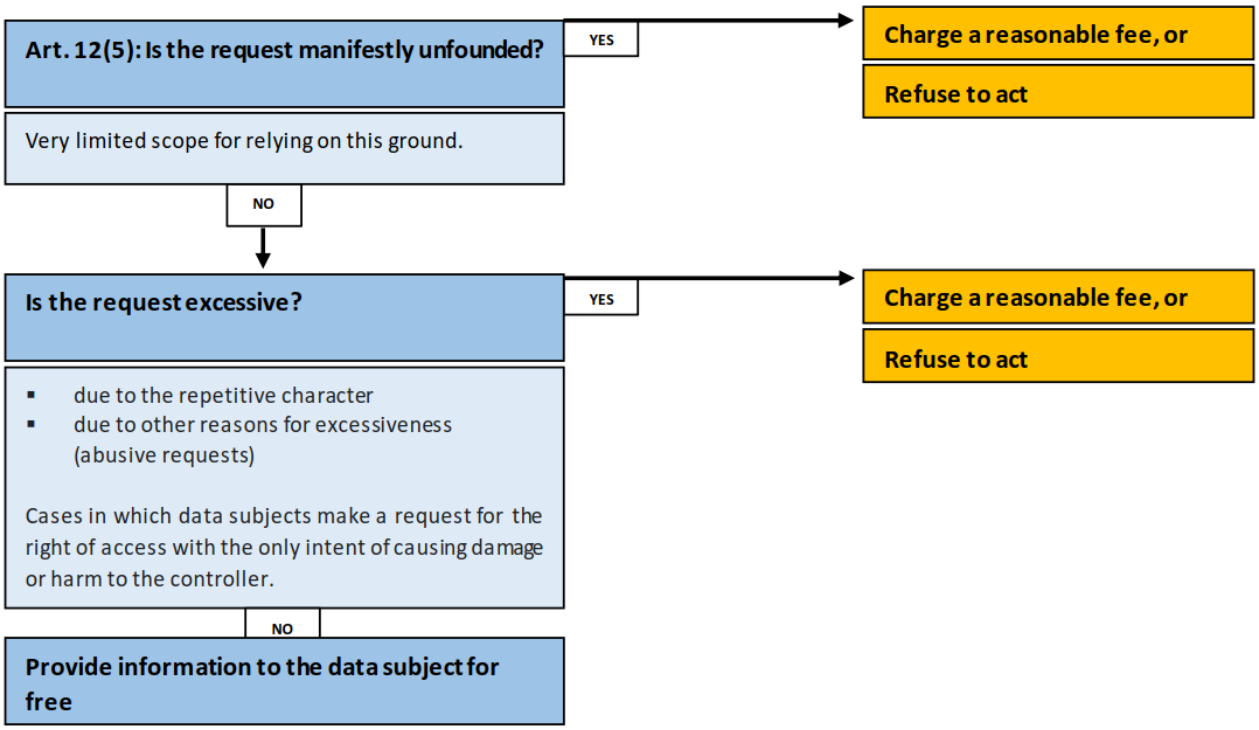


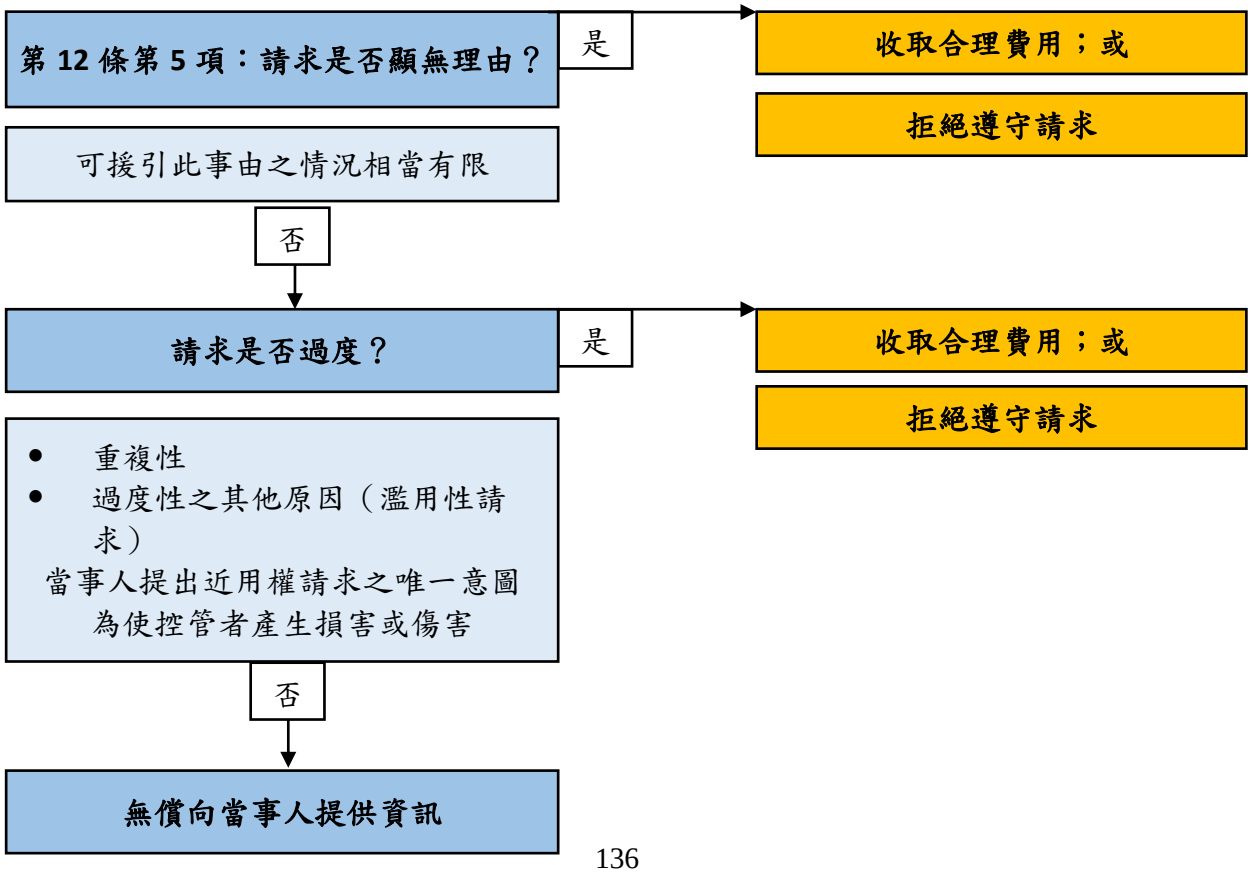
Step 3: Checking limits and restrictions (1)
第 3 步：確認限縮及限制(1)





Step 3: Checking limits and restrictions (2)
第 3 步：確認限縮及限制(2)





GDPR 相關指引文件研析/曾更瑩律師計畫主持;蕭秀玲律師協同主持.
-- 初版. -- 臺北市 : 國發會, 民 111.12
面：表，公分
編號：(111)018.0906
委託單位：國家發展委員會
受託單位：理律法律事務所
資訊法規
312.07

「GDPR 相關指引文件研析」委託研究計畫
委託單位：國家發展委員會
受託單位：理律法律事務所
計畫主持人：曾更瑩律師
協同主持人：蕭秀玲律師
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路 3 號
網址：http://www.ndc.gov.tw/
出版年月：中華民國 111 年 12 月
版次：初版
刷次：第 1 刷
編號：(111)018.0906 (平裝)