Article 29 Working Party

歐盟第 29 條工作小組

Adequacy Referential

適足性參考文件

Introduction

The Working Party of EU Data Protection Authorities[1](the WP29) has previously published a Working Document on transfers of personal data to third countries (WP12)[2]. With the replacement of the Directive by the EU General Data Protection Regulation (GDPR)[3], WP29 is revisiting WP12, its earlier guidance, to update it in the context of the new legislation and recent case law of the European Court of Justice (CJEU)[4].

引言

歐盟個資保護機關工作小組（下稱第 29 條工作小組）前曾發布關於傳輸個人資料至第三國之工作文件（下稱 WP12）。配合《一般資料保護規則（GDPR）》取代《個人資料保護指令》，第 29 條工作小組重新檢視先前指引文件 WP12，並依據新法規定及歐盟法院（下稱 CJEU）近期判例法更新其內容[5]。

---

[1] As established under Article 29 of the EU Data Protection Directive 95/46/EC
依歐盟第 95/46/EC 號指令第 29 條所成立。

[2] WP12 , 'Working Document: Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' adopted by the Working Part on 24 July 1998.
工作文件：將個人資料傳輸至第三國：適用 1998 年 7 月 24 日通過之歐盟個人資料保護指令第 25 條及第 26 條。

[3] 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) (Text with EEA relevance)
2016 年 4 月 27 日歐洲議會和理事會關於保護自然人個人資料處理和自由移動的法規（EU）2016/679，以及廢除第 95/46/ EC 號指令（一般資料保護規則）（與 EEA 相關的文本）。

[4] Including Case C‑ 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015
包含 2015 年 10 月 6 日 Case C-362/14，Maximillian Schrems 與資訊保護官一案之判決。

[5] 譯註：CJEU 實際上為歐盟最高法院，負責統一解釋歐盟法律與條約，其性質較接近美國最高法院或台灣司法院大法官解釋，其法律見解拘束歐盟會員國法院。

This working document seeks to update Chapter One of WP12 relating to the central question of adequate level of data protection in a third country, a territory or one or more specified sectors within that third country or in an international organization (hereafter: "third countries or international organizations"). This document will be continuously reviewed and if necessary updated in the coming years, based on the practical experience gained through the application of the GDPR. Chapters 2 (*Applying the approach to countries that have ratified Convention 108*) and 3 (*Applying the approach to industry self-regulation*) of the WP12 document should be updated at a later stage.

本工作文件旨在更新 WP12 第 1 章關於第三國、該第三國內之領域或一個或數個特定部門或國際組織（下簡稱第三國或國際組織）之個資保護適足程度核心問題。本文件未來將依 GDPR 生效適用後所獲得之實務經驗，持續檢視並於必要時更新。WP12 第 2 章（適用於已批准第 108 號公約的國家）及第 3 章（適用於產業自律規範）則於後續階段更新。

This working paper is focused solely on adequacy decisions, which are implementing acts[6] of the European Commission, according to article 45 of the GDPR. Other aspects of transfers of personal data to third countries and international organizations will be examined in following working papers that will be published separately (BCRs, derogations).

本工作文件專注於適足性認定說明，依據 GDPR 第 45 條，此項認定係歐盟執委會之施行法規。其他關於傳輸個人資料至第三國或國際組織之議題，將於後續工作文件中檢視，並另行發布（如拘束性企業規則、例外條款）。

This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations by establishing the core data protection principles that have to be present in a third country legal framework or an international organization in order to ensure essential equivalence with the EU framework. In addition, it may

[6] See relevant articles 45(3) and 93(2) of the GDPR for further information on the implementing acts
詳見 GDPR 第 45 條第 3 項及第 93 條第 2 項相關施行法。

guide third countries and international organizations interested in obtaining adequacy. However, the principles set out in this working document are not addressed directly to data controllers or data processors.

本文件之目的係依據 GDPR 規定，提供歐盟執委會與第 29 條工作小組評估第三國或國際組織之個資保護程度之指引，藉由建立第三國法律架構或國際組織中所應呈現之個資保護核心原則，以確保其法制架構實質等同於歐盟架構。此外，本文件亦得作為第三國或國際組織有意取得適足性認定之指引。然而，本工作文件所列原則並不直接適用於個資控管者或個資處理者。

The present document consists of 4 Chapters：

Chapter 1: Some broad information in relation to the concept on adequacy

Chapter 2: Procedural aspects for adequacy findings under the GDPR

Chapter 3: General Data Protection Principles. This chapter includes the core general data protection principles to ensure that the level of data protection in a third country or international organization is essentially equivalent to the one established by the EU legislation.

Chapter 4: Essential guarantees for law enforcement and national security access to limit the interferences to fundamental rights. This Chapter includes the essential guarantees for law enforcement and national security access following the CJEU Schrems judgment in 2015 and based on the Essential Guarantees WP29 working document adopted in 2016.

本文件包含以下 4 章：

第 1 章：關於適足性概念的概括資訊

第 2 章：GDPR 關於認定適足性的程序規定

第 3 章：一般資料保護原則。本章包含一般資料保護應具備之核心原則，以確保第三國或國際組織之個資保護程度與歐盟法規實質等同。

第 4 章：限制因執法及國家安全取得個資而妨礙基本權之實質保障。本章包含依據 2015 年 CJEU 對 Schrems 案之判決，凡因執法與國家

安全取得個資應具之實質保障，並以第 29 條工作小組於 2016 年通過之實質保障工作文件為基礎。

Chapter 1: Some broad information in relation to the concept of adequacy

第 1 章：關於適足性概念的概括資訊

Article 45, paragraph (1) of the GDPR sets out the principle that data transfers to a third country or international organization shall only take place if the third country, territory or one or more specified sectors within that third country or the international organization in question, ensures an adequate level of protection.

依 GDPR 第 45 條第 1 項規定，個資傳輸至第三國或國際組織，原則上僅限於該第三國、該第三國內之領域或一個或數個特定部門或國際組織確保個資保護適足程度時始得為之。

This concept of "adequate level of protection" which already existed under Directive 95/46, has been further developed by the CJEU. At this point it is important to recall the standard set by the CJEU in Schrems, namely that while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU, "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]"[7]. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

「適足保護程度」概念於第 95/46 號指令即已存在，且經 CJEU 進一步發展。此處應重申 CJEU 在 Shrems 案中建立的標準，亦即第三國的個資「保護程度」應與歐盟所保障者「實質等同」，但「第三國為達到該保護程度而採取之手段得與歐盟有別」。因此，符合適足性之目標並非逐項複製歐盟法律條文，而係建立該法律之實質-所謂的核心要件。

[7] Case C-362/14,Maximillian Schrems v Data Protection Commissioner,6 October 2015 (§§73,74); 見 Case C-362/14，Maximillian Schrems 與資訊保護官一案判決，2015 年 10 月 6 日，第 73 段及第 74 段。

The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States[8] that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union[9]. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules.

歐盟執委會的適足性認定之目的在於強制會員國，正式確認某第三國或國際組織之個資保護程度是否與歐盟實質等同。適足性達成包括個資當事人之權利、個資運用者或個資控管者之義務，以及獨立機關（構）的監督等整合措施而達成。然而，個資保護規範只有在該等規範具可執行性，且於實務上被遵循始能發揮效用。因此，有必要考量者，非僅個資傳輸至某第三國或某國際組織之規範內容，尚包含確保該等規範有效性之現有制度。有效之執法機制對個資保護規範之有效性至關重要。

Article 45, paragraph (2) of the GDPR, establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organization.

GDPR 第 45 條第 2 項，係規範歐盟執委會在評估某第三國或國際組織之個資保護程度適足性時應考量之要素。

---

[8] Article 288(2)TFEU
參歐盟運作條約第 288 條第 2 項。

[9] Case C-362/14,Maximillian Schrems v Data Protection Commissioner,6 October 2015 (§§52);
見 Case C-362/14，Maximillian Schrems 與資訊保護官一案判決，2015 年 10 月 6 日，第 52 段。

For example, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into.

例如，執委會應考量法律規範、對基本人權與自由之尊重、相關立法、是否存有一個或數個有效運作的獨立監管機關，及該第三國或國際組織簽署之國際承諾。

It is therefore clear that any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. It is upon the European Commission to verify – on a regular basis - that the rules in place are effective in practice.

由此顯見，任何對於適足保護有意義之分析，均應具備2項基本要素：適用規範之內容及確保有效適用之手段。該規範之有效實踐有賴歐盟執委會定期審核。

The 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the EU Charter of Fundamental Rights and the GDPR. In addition, consideration should also be given to other international agreements on data protection, e.g. Convention 108[10].

衍伸自歐盟基本權利憲章與 GDPR 之個資保護「內容」「核心」原則及「程序/執法」條件，可視為保護程度適足性的最低要求。此外，其他個資保護國際協定，例如第 108 號公約亦應納入考量。

Attention must also be paid to the legal framework for the access of public authorities to personal data. Further guidance on this is provided in

[10] Recital 105 of the GDPR
參 GDPR 前言第 105 點

Working paper 237 (i.e. the Essential Guarantees document)[11] on safeguards in the context of surveillance.

同時尚須留意公務機關取得個人資料之法律架構。對此，第 237 號工作文件（即實質保障文件）就採取監控之安全維護措施提供了進一步的指引。

General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable.

第三國僅具個資與隱私保護的一般規定並未充分符合適足性認定要件。相反的，第三國或國際組織之法律架構須具備特定相關規範，因應與個資保護權利實際相關之具體需求。而此類規範須具有可執行性。

Chapter 2: Procedural aspects for adequacy findings under the GDPR

第 2 章：GDPR 關於適足性評估審查之程序

For the EDPB to fulfil its task in advising the European Commission according to Article 70(1) (s) of the GDPR the EDPB should be provided with relevant documentation, including relevant correspondence and the findings made by the European Commission. Where the legal framework is complex, this should include any report prepared on the data protection level of the third country or international organization. In any case, the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country. The EDPB will provide an opinion on the European Commission's findings in due time and, identify insufficiencies in the adequacy framework, if any. The EDPB will also

[11] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP 237, 13 April 2016
個人資料傳輸時的監控措施對隱私與個資保護等基本權之干預的正當事由之工作文件 01/2016(歐盟實質保障)，第 237 號工作文件，2016 年 4 月 13 日。

endeavor to propose alterations or amendments to address possible insufficiencies.

歐洲個資保護委員會執行 GDPR 第 70 條第 1 項第 s 款規定之任務，對歐盟執委會之適足性評估提供意見，須取得評估相關參考文件，包含歐盟執委會與第三國或國際組織往來信函及其相關調查結果。該第三國或國際組織之法律架構複雜者，所提供之文件尚應包含其個資保護程度報告。總之，歐盟執委會應盡可能提供詳細資訊，俾歐洲個資保護委員會得自行對該第三國之個資保護程度作出評估。歐洲個資保護委員會將適時對歐盟執委會之調查結果表示意見，並指出其中適足性架構是否有不足之處。歐洲個資保護委員會亦將盡力提出調整或修正方案以為因應。

According to Article 45 (4) of the GDPR it is upon the European Commission to monitor – on an ongoing basis - developments that could affect the functioning of an adequacy decision.

依 GDPR 第 45 條第 4 項規定，應由歐盟執委會持續監督可能影響適足性認定運作之相關發展。

Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

GDPR 第 45 條第 3 項規定，至少每 4 年應執行定期審查。然而，此係一般性審查時間規定，仍須依個別第三國或國際組織的適足性認定予以調整。根據案件之特殊情況，亦可能准許採行較短的審查週期。再者，涉及該第三國或國際組織法律架構之事件、資訊或變動，亦可能衍生提前審查之需求。此亦顯示宜盡速先對全新之適足性認定(資格取得者)執行首次審查，再根據結果逐步調整審查週期間隔。

Given the mandate to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organization by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization. The EDPB would appreciate to be invited to participate in these review processes and missions.

歐洲個資保護委員會負有責任，對歐盟執委會就某第三國、該第三國內之領域或一個或數個特定部門或某國際組織是否不再具備適足個資保護程度提供意見，委員會因此應適時取得歐盟執委會監督該第三國或國際組織相關發展之有意義資訊。鑒此，任何對該第三國或國際組織之審查程序及審查任務，均應告知歐洲個資保護委員會。歐洲個資保護委員會將樂於受邀參與該審查程序與任務。

It should also be noted that according to article 45 (5) of the GDPR the European Commission has the right to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend should consequently involve the EDPB by requesting its opinion pursuant art. 70(1) (s).

亦應注意者，依 GDPR 第 45 條第 5 項規定，歐盟執委會有權撤銷、修正或暫停既存之適足性認定。該撤銷、修正或暫停程序必須依第 70 條第 1 項第 s 款規定，先請歐洲個資保護委員會表示意見。

Furthermore, as now recognized in article 58 (5) of the GDPR and according to the CJEU's Schrems ruling, data protection authorities must be able to engage in legal proceedings if they find a claim by a person against an adequacy decision well founded: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to

make a reference for a preliminary ruling for the purpose of examination of the decision's validity"[12].

再者，依 GDPR 第 58 條第 5 項規定，及根據 CJEU 於 Schrems 案之判決，個資保護機關如認當事人對適足性認定之申訴理由充分，必須能參與司法程序：「國家立法機構有責任提供法律救濟，俾國家監管機關能夠向國家法院提出適足性認定之異議，法院若對執委會認定之有效性亦有所質疑，則法院應請求（CJEU）做出檢驗該認定有效性之先決判決。」 。

Chapter 3: General Data Protection Principles to ensure that the level of protection in a third country, territory or one or more specified sectors within that third country or international organization is essentially equivalent to the one guaranteed by the EU legislation

第 3 章：一般資料保護原則，以確保第三國、該第三國內之領域或一個或數個特定部門或國際組織之個資保護程度實質等同於歐盟法律

A third country's or international organisation's system must contain the following basic content and procedural/enforcement data protection principles and mechanisms:

第三國或國際組織之制度應包含下列基本內容與個資保護程序/執行之原則與機制：

A. Content Principles：內容原則

1)Concepts

Basic data protection concepts and/or principles should exist. These do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data".

1)概念

[12] Case C-362/14,Maximillian Schrems v Data Protection Commissioner,6 October 2015 (§65)
見 Case C-362/14，Maximillian Schrems 與資訊保護官一案判決，2015 年 10 月 6 日，第 65 段。

須具備基本個資保護概念及/或原則。此概念及/或原則雖無須與GDPR用語完全相同，但應能反映且符合歐盟個資保護法闡釋之概念。舉例而言，GDPR包含下列重要概念：「個人資料」、「個人資料運用」、「個資控管者」、「個資受託運用者」、「接受者」及「敏感個資」等。

2)Grounds for lawful and fair processing for legitimate purposes

Data must be processed in a lawful, fair and legitimate manner.

The legitimate bases, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

2)為正當目的而合法、公平運用個資之依據

個資運用應以合法、公平且正當之方式為之。

應以足夠清晰之方式說明合法、公平且正當運用個資的法律依據。歐盟架構承認之數項正當事由，包含例如國家法律規定、個資當事人同意、為履行契約或為個資控管者或第三人之正當利益，且該利益並未逾越該個資當事人之利益。

3)The purpose limitation principle

Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

3)目的拘束原則

個資運用應基於特定目的，且後續之利用行為僅得於與運用目的相符之範圍內為之。

4)The data quality and proportionality principle

Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

4)個資品質與比例原則

個資之正確性應予維護，必要時並應持續更新。個資之運用應適當、並與運用目的相關，且不逾越該運用目的之必要範圍。

5)Data Retention principle

Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed.

5)個資保存原則

原則上，個資保存期間不得逾運用目的所需之必要期間。

6)The security and confidentiality principle

Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

6)安全與保密原則

任何運用個資之實體均應確認，係以確保該個資安全之方式加以運用，包含採取適當之技術性或組織性措施，以防止未獲授權或非法之運用，意外遺失、毀壞或損害。所採取之安全措施等級並應考量最新技術水平及相關成本。

7)The transparency principle

Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise, transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is

necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

7)透明原則

應以清楚、易於取得、簡潔、透明及易懂之方式，告知個別個資當事人運用其個資之所有主要要素。告知之資訊應包含運用之目的、個資控管者之身分、當事人可行使之權利，以及為確保公平性之其他必要資訊。於某特定情形下，前述資訊請求權得有例外，例如維護刑事偵查、國家安全、司法獨立，以及司法程序或 GDPR 第 23 條所列其他一般公共利益之重要目的。

8)The right of access, rectification, erasure and objection

The data subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed.

The data subject should have the right to obtain rectification of his/her data as appropriate, for specified reasons, for example, where they are shown to be inaccurate or incomplete and erasure of his/her personal data when for example their processing is no longer necessary or unlawful.

The data subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. In the GDPR, for example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

The exercise of those rights should not be excessively cumbersome for the data subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

8)近用、更正、刪除及拒絕等權利

個資當事人應有權確認其個資是否正被運用，並有權接近使用其個人資料，包含取得一份所有其被運用個資之複製本。

個資當事人應有權於特定理由下，例如其個資經顯示不正確或不完整時，適當更正其個人資料；且於例如個資運用已無必要或不合法時，請求刪除其個資。

個資當事人基於迫切正當之理由，應有權隨時拒絕以第三國法律架構下之特定要件對其個資之運用。以 GDPR 為例，前述特定要件包含為公共利益而執行職務所必要、為行使公務機關賦予控管者之權力所必要，或為個資控管者或第三人追求正當利益所必要。

個資當事人行使上述權利之程序不宜過於繁瑣。此等權利之行使得設有限制，例如為維護刑事偵查、國家安全、司法獨立，以及司法程序或 GDPR 第 23 條所列其他一般公共利益之重要目的。

9)Restrictions on onward transfers

Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.

9)再傳輸之限制

個資由原傳輸之接收者再傳輸時，僅於再接收者（再傳輸之接收者）亦符合個資保護適足性規範（包含契約規範），且於受託為個資控管者運用個資時，遵守（個資控管者）相關指示者，始得為之。對於個資被傳輸之自然人之保護程度不得於再傳輸中有所減損。取得歐盟個資之原接收者，應負責確保該個資再傳輸至尚未取得適足性認定資格者時，獲得適當的保護。此等個資之再傳輸應僅限少數特定之目的且合法之情形下，始得為之。

B. Examples of additional content principles to be applied to specific types of processing：

B. 其他適用於特定運用類型的內容原則例示：

1)Special categories of data

Specific safeguards should exist where 'special categories of data are involved [13]. These categories should reflect those enshrined in Article 9 and 10 of the GDPR. This protection should be put in place, through more demanding requirements for the data processing such as for example, that the data subject gives his/her explicit consent for the processing or through additional security measures.

1)特種個資

涉及特種個資時，應有特定的安全維護措施。所謂特種個資應符合 GDPR 第 9 條及第 10 條規範之類型。此種保護應透過更多高標準之個資運用要件予以落實，例如應經個資當事人明確同意，或透過額外之安全措施達成。

2)Direct marketing

Where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time.

2)直效行銷

[13] Such special categories are also known as "sensitive" in recital 10 of the GDPR.
所稱「特種」個資在 GDPR 前言第 10 點亦稱為「敏感」個資。

個資當事人應得隨時拒絕以直效行銷為目的之個資運用且無須負擔任何費用。

3)Automated decision making and profiling

Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. In the European framework, such conditions include, for example, the need to obtain the explicit consent of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. The law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis.

3)自動化決策及剖析

基於自動化運用（自動化個別決策），包含剖析，而對個資當事人產生法律效力或重大影響之決策，僅得於符合第三國法律架構之特定要件時始得為之。在歐盟架構中，此類要件包含例如取得個資當事人的明確同意，或該決定係為契約成立所必要。若該決策之作成並未遵循第三國法律架構所規定之要件時，個資當事人應有權不受拘束。在任何情況下，該第三國法律應提供必要之保護措施，包含個資當事人有權受告知作成該決策之具體理由及相關邏輯、更正不正確或不完整之資訊，以及對根據不正確事實作出之決策提出異議。

C. Procedural and Enforcement Mechanisms：

C.程序與執行機制：

Although the means to which the third country has recourse for the purpose of ensuring an adequate level of protection may differ from those

employed within the European Union[14], a system consistent with the European one must be characterized by the existence of the following elements：

第三國確保個資保護適足程度所採取之手段固得與歐盟不同，惟符合歐盟標準之制度仍須具備以下要件：

1) Competent Independent Supervisory Authority

One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.

1) 適當之獨立監管機關

第三國應設置一個或數個獨立監管機關，賦予監督、確保並執行個資與隱私保護法規遵循的任務。該監管機關應完全獨立、公正執行職務與行使權力，因此亦不得尋求或接受任何人指示。在此情形下，監管機關為確保遵循個資保護權利並提升認知，應被賦予所有必備之權力與職責。同時應考量給予該監管機關所屬的人員編制與預算。該監管機關亦應得主動進行調查。

2) The data protection system must ensure a good level of compliance

A third country system should ensure a high degree of accountability and of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The

[14] Case C-362/14,Maximillian Schrems v Data Protection Commissioner,6 October 2015,para.74.
參 Case C-362/14，Maximillian Schrems 與資訊保護官一案判決，2015 年 10 月 6 日，第 74 段。

existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

2) 個資保護制度須確保良好的法規遵循程度

第三國制度應確保具備高度之課責性，並確保個資控管者與為其運用個資之人對其義務、工作與責任，以及個資當事人對其權利與行使方式，均有高度認知。有效且有嚇阻力之裁罰，以及主管機關、稽核員或獨立個資保護官員直接檢驗制度，均對確保法規遵循有舉足輕重之影響。

3) Accountability

A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.

3) 課責性

第三國個資保護架構應課予個資控管者及/或為其處理個資者責任，須遵循其規範，並有能力向適當監管機關證明其合規性。其措施得包含例如個資保護衝擊評估、保存適當期間內個資運用之紀錄或軌跡、指派個資保護長，或個資保護之設計與預設。

4) The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and

enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.

Where rules are not complied with, the data subject should be provided as well with effective administrative and judicial redress, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

4) 個資保護機制應對個別個資當事人行使權利提供支援與協助，及適當的救濟機制

當事人應能迅速、有效、低成本的尋求法律救濟以行使其權利，並確保法規遵循。為此，應建置監督機制就相關申訴進行獨立調查，並使任何侵害個資保護權利及隱私之行為皆被識別及處罰。

當法規未被遵循時，應提供個資當事人有效之行政與司法救濟，包含對非法運用其個資所致之損害賠償。此關鍵要素必須涵蓋獨立裁決或仲裁之制度，俾當事人得獲賠償，侵害者得受適當裁罰。

Chapter 4：Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights

第 4 章：限制因執法及國家安全取得個資而妨礙基本權之實質保障

When assessing the adequacy of the level of protection, under Art 45(2)(a) the Commission is required to take into account "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation…".

評估保護程度之適足性時,歐盟執委會依據第 45 條第 2 項 a 款規定，應考量「相關的普通法與特別法，包含涉及公共安全、國防、國家安全、刑法及公務機關取得個人資料之法律與該等法律之執行…」。

The CJEU in Schrems, noted that the "term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of

protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter".

CJEU 於 Schrems 案中指出，「『保護之適足程度』一詞應理解為要求第三國以其內國法或國際承諾，確保其對基本權與自由之保護程度，與歐盟第 95/46 號指令依憲章解釋所保障者實質等同」。

Even though the means to which that third country has recourse, in this connection, may differ from those employed within the European Union, those means must nevertheless prove, in practice, effective[15].

儘管第三國與歐盟採取之保護手段或有不同；實務上，其所採手段仍須證明為有效可行。

In this context, the court also noted critically that the previous Safe Harbor decision did "not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security."

在此背景下，法院亦嚴正指出，先前歐盟與美國之安全港決議「並未發現美國採行任何法律，對其政府機關經授權而以例如國家安全之正當目的，於自然人個資由歐盟傳輸至美國時，干預其基本權之行為予以限制」。

The WP29 has identified in the opinion WP237, adopted on 13 April 2016, essential guarantees reflecting the jurisprudence of the CJEU and the ECHR in the field of surveillance. While the recommendations detailed in WP237 remain valid and should be taken into account when assessing the adequacy of a third country in the field of surveillance, the application of these guarantees may differ in the fields of law enforcement and national security access to data. Still those four guarantees need to be respected for access to data, whether for national

[15] See recital 74 of Case C-360/14 "Schrems"
參 Case C-360/14(譯注：似為 C-362/14 誤植) Schrems 案判決第 74 段。

security purposes or for law enforcement purposes, by all third countries in order to be considered adequate：

1) Processing should be based on clear, precise and accessible rules (legal basis)

2) Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated

3) The processing has to be subject to independent oversight

4) Effective remedies need to be available to the individuals

第 29 條工作小組於 2016 年 4 月 13 日通過之 WP237 號意見中載明之實質保障，正反映歐盟法院與歐洲人權法院關於監控之法理。WP237 中詳列的建議有效，且應於評估第三國監管之適足性時一併考量的情況下，在因執法或國家安全而取得個資之領域內，所適用之保障方式得有不同。然而，所有第三國無論是基於國家安全或執法目的取得個資，凡欲取得適足性認定資格，仍應遵循下列 4 項保障要件：

1) 個資運用應基於清楚、明確且公開之法規（法律依據）

2) 須證明達成正當目的之必要性與合比例性

3) 個資運用應受獨立監督

4) 應予當事人有效之救濟