歐盟 GDPR 適足性相關文件與判決之
對外說明資料
結案報告

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 107 年 12 月 24 日

歐盟 GDPR 適足性相關文件與判決之對外說明資料

結案報告

受委託單位：達文西個資暨高科技法律事務所

研究主持人：葉奇鑫律師

研 究 期 程 ：107 年 8 月 28 日至 107 年 10 月 31 日

研 究 經 費 ：新台幣壹拾萬元整

國家發展委員會 委託研究

中華民國 107 年 10 月

目錄

壹、研究說明

本研究係對歐盟個資保護機關工作小組（第 29 條工作小組）發布的 WP254 號文件（適足性參考）提出說明與翻譯；並對歐盟法院的 Schrems 案判決提出說明、評析及翻譯。

WP254 號文件及歐盟法院的 Schrems 案判決均對歐盟執委會在認定第三國的個資保護程度是否具備適足性，而得列入「可將歐盟公民個資自歐盟傳輸至該第三國」的白名單時，所應考量該第三國法制的關鍵要素提出說明，並對歐盟執委會有拘束效力。

是本研究於第貳章說明 WP254 號文件之內容、於第參章說明並評析歐盟法院的 Schrems 案判決，並將 WP254 號文件的中英文對照翻譯列為附件 1、將歐盟法院的 Schrems 案判決之中英文對照翻譯列為附件 2。

貳、WP254 號文件說明

一、文件目的

歐盟個資保護機關工作小組（第 29 條工作小組）前於 1998 年發布關於傳輸個人資料至第三國之工作文件（WP12），但隨著歐盟《個人資料保護指令（95/46/EC）》經《一般資料保護規則（GDPR）》取代，以及歐盟法院（CJEU）於 Schrems 案作出的判決出爐，第 29 條工作小組重新檢視該 WP12 號文件並更新內容，最終發布本 WP254 號文件（最新修訂版本於 2018 年 2 月 6 日發布）。

本文件旨在更新 WP12 號文件第 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，即聚焦於歐盟執委會對第三國或國際組織作成的「（個資保護程度）適足性決定」。

因此，本文件目的在於提供歐盟執委會與第 29 條工作小組依據 GDPR 對第三國或國際組織之個資保護程度進行評估之指引，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。

同時，本文件亦得作為有意取得適足性認定之第三國或國際組織的指引。

二、文件重點

（一） 適足性概念的概括資訊

本文件指出，雖然第三國的「（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方式可與歐盟有別」。因此，目標並非逐項複製歐盟法律條文，而應建立該法律的核心規範。

適足性可經由結合個資當事人之權利、課予處理個資者或對處理行為執行控管者之義務，及獨立機關（構）的監督等面向而實現。然而，個資保護規範只有在該等規範具備可執行性且於實務上被遵循始能發揮效用。

因此，歐盟執委會有必要考量者，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。即任何對於適足保護程度有意義之分析均應包含 2 項基本要素：「適用規範之內容」及「確保有效適用之方法」；且歐盟執委會應定期審核該規範是否有效實踐。

（二） 適足性調查之程序

本文件再指出，依 GDPR 第 45 條第 4 項規定，歐盟執委會應持續監督可能影響適足性決定功能之相關發展；且依 GDPR 第 45 條第 3 項規定，至少每 4 年應對適足性決定執行

定期審查。然而，此僅為一般性的時間規定，必須依個別第三國或國際組織的適足性決定調整。根據當時的特殊情況，亦可能認定較短的審查週期。再者，該第三國或國際組織之事故或涉及法律架構之資訊或變動，亦可能導致提前審查之需求。

且依依 GDPR 第 58 條第 5 項規定，及根據歐盟法院於 Schrems 案之判決，歐盟會員國之個資保護機關如認當事人對適足性決定之申訴理由充分，必須能參與法律程序。

最後，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決定。

（三） 確保第三國或國際組織之個資保護程度實質等同於歐盟法律的一般資料保護原則

本文件認為，第三國之法律規範應至少包含數項基本概念或原則，始能最低程度使個資當事人獲得的保障與歐盟法律規範實質等同，例如「正當性原則（合法、公平處理個資）」、「目的限制原則」、「個資品質與比例原則」、「個資保存原則」、「安全與保密原則」、「透明原則」、「當事人權利保障原則」、「再傳輸限制原則」等。

此外，為確保該第三國法律規範能有效實踐，該第三國在個資保護制度上應設有適當的獨立監管機關；且應能確保個資

控管者與為其處理個資之人對其義務、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；亦應具備有效且有嚇阻力之裁罰；並建立由主管機關、稽核員或獨立個資保護官員直接檢驗之制度。

又第三國的個資保護制度應課予個資控管者及/或為其處理個資之人遵循規範並證明合規性的義務。

另在當事人救濟制度方面，第三國的個資保護制度應使當事人能迅速、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，第三國應設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尊重私人生活之行為皆被識別及處罰。

又當法規未被遵循時，第三國的個資保護制度應提供個資當事人有效之行政與司法救濟，包含對違法處理其個資所致之損害賠償。

（四） 必要保障以限制因執法及國家安全取得個資而妨礙基本權

最後，本文件認為，參酌歐盟法院於 Schrems 案判決之見，歐盟執委會在評估第三國的個資保護程度之適足性時，應一併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情形。

對此，第三國無論基於國家安全或執法目的，於取得個資時，仍應注重下列 4 種保障內容：

1、 個資處理應基於清楚明確、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、 個資處理應受獨立監督。

4、 應予當事人有效之救濟。

參、歐盟法院 Schrems 案判決說明與評析

一、背景—歐盟執委會第 2000/520 號決定：安全港架構

無論是 1995 年生效的歐盟《個人資料保護指令（95/46/EC）》（以下稱個資保護指令）或 2018 年 5 月 25 日生效以取代個資保護指令的歐盟《一般資料保護規則（General Data Protection Regulation, GDPR）》，歐盟個資保護法律對於「將歐盟自然人之個資由歐盟境內傳輸至境外第三國或國際組織」之行為，皆規範原則上僅於該第三國或國際組織的個資保護程度具備經歐盟執委會認可的「適足性（adequacy）」時，始得為之。

個資保護指令第 25 條第 6 項規定，歐盟執委會考量第三國的內國法或簽署的國際承諾，得認定該第三國對於私人生活及個人基本權利與自由的保護達到適足程度，而符合指令要求的適足性。

於 2000 年，歐盟執委會於即依個資保護指令第 25 條第 6 項規定，作出第 2000/520 號決定（Decision 2000/520），承認歐美間的「安全港隱私保護原則（Safe HarbourPrivacy Principles）」（以下稱安全港原則），即自我證明（seld-certified）遵守「安全港原則」及「美國商務部於 2000 年 7 月 5 日就如何遵守安全港

原則發布的常見問答（FAQs）」的美國組織，視同符合個資保護指令的「適足性」要件，而得接受歐盟境內傳輸之個人資料。

13 年後，歐盟執委會於 2013 年發布「重建歐美資料流動信任（Rebuilding Trust in EU-US Data Flows）」文件（COM(2013) 846 final)），其中的調查報告係在美國遭揭露存在大規模蒐集個人資料的監控計畫後，歐盟與美國合作調查之成果，內容包括美國法律的詳細分析，特別是監控計畫及美國政府蒐集和處理個人資料的法源依據。

文件指出，依安全港原則而傳輸至美國的歐洲公民之個資，可能會被美國政府以不符合該資料自歐盟蒐集之原始目的，或該資料傳輸至美國之目的而使用與處理，即美國多數涉及政府監控計畫的網路公司均通過安全港原則而獲得適足性認證，但卻都受到美國政府監控計畫的拘束，而將歐盟公民的個資提供美國政府存取。此無異使得安全港原則成為美國政府（尤其是情報機構）取得歐洲公民個資的管道。文件最終則表示，歐盟將持續與美國就此缺失展開檢討。

然而在 2015 年，歐盟法院（Court of Justice of the European Union, CJEU）[1]於 Schrems v. Data Protection Commissioner 案（以下稱 Schrems 案）中宣告該 2000/520 號決定失效，使歐美雙方必須重新建置跨境傳輸的適當法律架構。

二、Schrems 案事實

本案係 Schrems 與愛爾蘭資訊保護官（Data Protection Commissioner）間，針對後者駁回 Schrems 訴請調查臉書愛爾蘭有限公司（下稱臉書愛爾蘭公司）將用戶個人資料跨境傳輸至美國並保存於當地伺服器一案所提出。

Schrems 為奧地利籍公民，自 2008 年起成為臉書之用戶。任何欲使用臉書的歐盟居民，須在其註冊時與臉書愛爾蘭公司成立契約，而該公司的母公司（即臉書公司）係設於美國。臉書愛爾蘭公司於歐盟境內儲存的用戶部分或全部個資，皆經傳輸至位於美國臉書母公司之伺服器進行處理。

2013 年 6 月 25 日，Schrems 向愛爾蘭資訊保護官申訴，要求其行使法定權力，調查臉書愛爾蘭公司傳輸其個資至美國的行為。依 Schrems 的主張，美國法律之規定與執行無法確保對於個

[1] CJEU 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。

人資料具備適足保護程度以防止政府的監控，並於此提及愛德華·史諾登(Edward Snowden)所揭露美國情報機構的監控行為。

資訊保護官認為並無義務調查 Schrems 提出的申訴，遂以該案無事實根據而駁回。資訊保護官認為，並無事證顯示 Schrems 之個資已為美國國家安全局（NSA）取得，且基於歐盟執委會第 2000/520 號決定，美國個資保護適足性已由歐盟執委會依決定內容予以確認，因此無法受理 Schrems 的申訴。

於是，Schrems 對資訊保護官的決定（非針對第 2000/520 號決定）提起法律救濟。愛爾蘭高等法院認為，雖然 Schrems 未對個資保護指令或 2000/520 號決定之有效性提出質疑，但本案關鍵在於資訊保護官「是否受歐盟執委會依個資保護指令第 25 條第 6 項規定，對於美國確保具備個資保護適足性而作出的第 2000/520 號決定所拘束」，或依歐盟基本權利憲章第 8 條之意旨，資訊保護官於適當時可不受上述決定之拘束。

因此，愛爾蘭高等法院停止訴訟程序，將本案提交歐盟法院針對以下爭點為先決判決（preliminary ruling）[2]：

[2] 在歐盟，Preliminary ruling 係指歐盟會員國法院於訴訟中遇有涉及歐盟法律（或條約）之解釋爭議時，先暫停訴訟，並聲請 CJEU 做出先決判決，該先決判決為該歐盟法律之終局解釋，不僅拘束聲請解釋之法院，並拘束所有歐盟會員國法院，但該案件仍由聲請法院於接獲先決判決之解釋後，為最終判決。

獨立行使個資保護管理與執法權的資訊保護官，在處理『個資當事人主張其個人資料被傳輸至第三國（於本案即指美國），而該國法律之規定與執行對個資當事人缺乏適足保護之申訴』時，如該國已符合第 2000/520 號決定而滿足適足性要求(即與當事人之主張相悖),則資訊保護官是否依歐盟基本權利憲章第 7 條、第 8 條和第 47 條及個資保護指令第 25 條第 6 項規定，仍受第 2000/520 號決定之拘束？抑或資訊保護官得或須依具體事實自行展開調查？

三、歐盟法院判決

歐盟法院於審理後作出下列認定：

（一） 針對愛爾蘭高等法院提出之爭點

歐盟法院認為，依個資保護指令第 28 條規定，歐盟會員國須設立一個或多個獨立機關，負責監管個資處理行為，此一要求係源自於歐盟的主要法律，即基本權利憲章第 8 條及歐盟運作條約（TFEU）第 16 條。國家監管機關尤其應確保隱私權的遵守及個人資料自由流動利益兩者間之平衡。為達此一目的，國家監管機關應有對應的權力，例如調查權（即為履行該監督職責而有權蒐集所有資訊）、處分權（即對個人資料處理施以暫時或終局禁令），或有權進行訴訟。因此，國家監管機關應

有權查核自該國向第三國傳送個資之行為是否符合個資保護指令的要求。

亦即，歐盟執委會之決定不能阻礙個資當事人依個資保護指令第 28 條第 4 項規定向國內監督機關提出申訴之權，即便申訴標的為依該指令第 25 條第 6 項通過之決定亦不例外，即歐盟執委會的決定不可有違或減損歐盟基本權利憲章第 8 條及個資保護指令第 28 條賦予國家監管機關的權力，因此，即便是針對歐盟執委會之決定，當國家監管機關受理涉及處理個資之權利及自由的申訴時，必須能完全獨立的檢視個資傳輸是否符合個資保護指令規範。

倘非如此，對於個資已經或可能移轉至第三國之當事人，無異剝奪其得依歐盟基本權利憲章第 8 條向國家監督機構申訴保護基本權利之權。

據此，歐盟執委會雖依個資保護指令第 25 條第 6 項規定作成第 2000/520 號決定，認定第三國（美國）得確保個資保護的適足程度，但並不阻礙會員國之監管機關依該指令第 28 條規定，受理（並調查）個資當事人對該第三國之法律規定與執行的保護程度不足之申訴。

（二） 針對歐盟執委會第 2000/520 號決定的效力

然而，歐盟法院認為，歐盟執委會依個資保護指令第 25 條第 6 項規定，作出第三國保護程度具備適足性之決定，依該指令第 25 條第 6 項第 2 款規定，會員國須採取必要措施以遵守該決定；又依歐洲聯盟運作條約第 288 條第 4 項規定，該決定之效力效力將拘束所有會員國及其相關組織。因此，在該決定被法院宣告無效之前，所有會員國及其組織，包含其所屬之獨立機關，均無法否認該決定的有效性。

因此，既然 Scherms 係主張美國法律的規定與執行並無法確保歐盟個資保護指令規範下的個資保護適足程度，本案關鍵即在於歐盟執委會第 2000/520 號決定的有效性。為完整解決本案紛爭，歐盟法院即續對該決定是否滿足個資保護指令之規範具體審查。

歐盟法院首先指出，依個資保護指令第 25 條第 6 項文義解釋觀之，受該執委會決定效力所及的第三國應承擔確保個資保護程度適足性的法律義務，即便第三國為達到適足程度之保護所採取的方式或異於歐盟，其方式仍須有效使得該國的個資保護程度與歐盟所保障者實質相同。因此，歐盟執委會在審查第三國的個資保護程度時，即須考量該第三國內國法律或國際

承諾的內容，以及確保受規範主體如實遵循相關規範的執行措施。

又鑒於第三國之個資保護程度發生變動的可能，歐盟執委會亦應在依個資保護指令第 25 條第 6 項通過決定後，定期檢視該第三國所保證的個資保護程度是否在事實上及法律上仍屬有據；並且，在檢視決定有效性時，歐盟執委會應一併考量在決定通過後發生的所有情況。

其次，歐盟法院認為，依歐盟執委會第 2000/520 號決定第 1 條第 1 項規定，美國組織如自我證明遵循由美國商務部發布的安全港原則(該決定附件 1)及常見問答(該決定附件 2)，即可符合歐盟要求的個資保護適足程度。

但由該決定附件 1（安全港原則）第 2 段可知，安全港原則並非強制手段，而僅係由美國組織自願選擇是否導入，以符合歐盟就跨境傳輸個資所要求的個資保護程度適足性。因此，美國的政府機關並無義務遵循該安全港原則。

此外，第 2000/520 號決定第 2 條說明本決定僅考量美國在安全港原則下的個資保護適足程度符合個資保護指令第 25 條第 1 項的要求，但並未於決定中載明歐盟執委會已按個資保

護指令第 25 條第 6 項規定，認定美國依內國法或簽署之國際承諾所採取的何種措施得以確保個資保護的適足程度。

且依第 2000/520 號決定附件 1(安全港原則)第 4 段可知，自我證明符合安全港原則的美國組織在面臨「國家安全、公共利益或執法要求」，或「依法律、政府規則或法院判決而有義務衝突或明確授權的情形」時，得不遵守安全港原則。對此，該決定於附件 4 的 B 部指出，當美國法律對美國組織產生衝突義務時，美國組織無論是否導入安全港原則，均應優先遵守美國法律。

除此之外，該決定亦未包含當美國政府以前述理由造成歐洲公民的基本權利與自由之干預時，有無任何法律限制或有任何法律得防止此種干預。即美國政府能取得自歐盟會員國傳輸之個人資料，並以保護程度不足的方式處理該資料，且個資當事人並無任何行政或司法救濟手段。如此侵害基本權利與自由之行為，與歐盟基本權利憲章相悖。

因此，無需審查安全港原則的內容，便可認定歐盟執委會第 2000/520 號決定第 1 條因不符個資保護指令第 25 條第 6 項規定及歐盟基本權利憲章，因而無效。

最後，依歐盟基本權利憲章第 8 條及個資保護指令第 28 條規定，國家監管機關必須能夠獨立審查任何個資當事人對其權利及自由之申訴，尤其包含個資當事人對於歐盟執委會依個資保護指令第 25 條第 6 項通過之決定是否足以保護其隱私權、基本權利與自由之質疑。

但依歐盟執委會第 2000/520 號決定第 3 條第 1 項規定，國家監管機關僅得於特定條件下「暫停」個資跨境傳輸至自我證明符合安全港原則的美國組織，此規定將排除國家監管機關依個資保護指令第 28 條所得行使之完整權力，惟歐盟個資保護指令第 25 條第 6 項賦予歐盟執委會的權力並不包含有權限制國家監管機關的權力。

因此，第 2000/520 號決定第 3 條規定已逾越歐盟基本權利憲章及個資保護指令，亦應無效。

綜合上述見解，歐盟法院認為，由於歐盟執委會第 2000/520 號決定第 1 條、第 3 條與第 2 條、第 4 條及其附件（安全港原則、常見問答等）無法分割，因此其無效性及於全體，是該第 2000/520 號決定應全部無效。

四、安全港之後—歐盟第 2016/1250 號決定：隱私盾（Privacy Shield）架構

在安全港原則依附的第 2000/520 號決定被歐盟法院宣告無效後，歐盟與美國政府續就替代的跨境傳輸個資適足性法律架構進行協商，終在 2016 年 7 月，歐盟執委會通過第 2016/1250 號決定，宣布美國政府提出的「隱私盾（Privacy Shield）」法律架構，足以滿足個資保護指令要求的個資保護程度之適足性。該決定重點如下：

（一）該決定第 1 條第 1 項即明示，在隱私盾框架下，美國得以確保自歐盟傳輸至美國組織的個人資料獲得適足程度的保護；同條第 3 項並說明，美國商務部將維護並公開「隱私盾清冊（Privacy Shield List）」，記載符合隱私盾框架的美國組織名單。而依同條第 2 項所述，所謂「隱私盾」即包含由美國商務部發布並列於該決定附件 2 的「隱私盾原則」，以及其他列為附件的官方陳述與承諾。

（二）該決定第 2 條則謂，該決定不影響個資保護指令第 25 條第 1 項（即跨境傳輸個資的適足性條件）以外之其他規定於歐盟會員國內的適用。

（三）又該決定第 3 條規定，歐盟會員國的主管機關在行使個資保護指令第 28 條第 3 項賦予之權力，並將基於保護當事人之目的而暫停或終止個人資料傳輸至列於隱私權清冊中的美國組織時，該會員國應即時將此事通知歐盟執委會。

（四）另該決定第 4 條第 1 項表明，歐盟執委會將持續評估美國是否得確保自歐盟傳輸至美國組織的個人資料獲得適足程度的保護，以監督隱私盾法律架構的功能。

（五）同條第 2 項則規定，當歐盟會員國或執委會發現，具有法律權力得要求組織遵循隱私盾原則的美國政府機構，竟無法提供有效的偵測與監督機制以識別組織違反該原則之情事並予處罰時，應互相通知；第 3 項復規定，當歐盟會員國或執委會發現任何跡象，顯示美國執掌國家安全、法律執行或其他公共利益的公務機關對於當事人個資保護權利的干預已超過必要範圍，且／或對該干預並無有效的法律得予保障時，亦應互相通知。

（六）同條第 4 項並要求，在將該決定通知各會員國之日一年後（之後亦每年執行），歐盟執委會將根據所有可得之資訊，包含依本決定附件規定所做的「年度聯合審查（Annual Joint Review）」，再次評估該決定第 1 條第 1 項所稱「在隱私盾框架下，美國得

以確保自歐盟傳輸至美國組織的個人資料獲得適足程度的保護」之認定。

（七）最後，該決定第 6 條說明，當有跡象顯示下列情況發生時，歐盟執委會將依個資保護指令規範之程序提出議案，以中止、修正或撤銷本決定，或限縮其範圍：

1、美國公務機關並未遵守列於本決定附件之官方陳述或承諾，包含美國公務機關為執法、國安及其他公益目的而存取經由隱私盾傳輸至美國之個人資料的條件或限制。

2、無法有效因應歐盟個資當事人之申訴。

3、隱私盾監察人（Privacy Shield Ombudsperson）無法即時並適當地依該決定附件 3 之規定，回應歐盟個資當事人的請求。

4、由於得確保隱私盾功能之美國機構的不合作，而使歐盟執委會難以判斷該決定第 1 條第 1 項所稱「在隱私盾框架下，美國得以確保自歐盟傳輸至美國組織的個人資料獲得適足程度的保護」之認定是否受影響。

五、隱私盾原則

在隱私盾法律架構下，仍係由美國組織自行導入隱私盾之各項原則，並提出自我證明表示已遵守符合該架構之要求。其主要七大原則概述如下：

（一）告知義務

此原則規範個資控管者的應告知事項及告知時機，包含蒐集的個資類別、蒐集目的、遵守隱私盾的承諾、當事人權利及行使管道、擬揭露個資的對象及目的、當事人得限制資料使用或揭露的選擇權與行使方式、該個資控管者受到美國相關主管機關管理等。

（二）當事人選擇權

此原則要求個資控管者提供當事人選擇拒絕（Opt-Out）「資料被揭露予第三人」或「資料被用於與原始蒐集目的重大不符之新目的」的權利。

（三）資料再傳輸責任

如個資控管者欲將個資再傳輸予第三人，須遵守前述告知義務與當事人選擇權原則，並應以契約要求該第三人僅得於當事人同意的特定目的限制內使用當事人個資，且要求第三人以同樣程度遵守隱私盾原則。

如個資控管者欲將個人資料傳輸予受託處理個資的個資處理者時，個資控管者僅得在原始蒐集個資之目的限制內為之，且須確保受託者的個資保護措施應至少遵守隱私盾規範，並應採取合理的適當措施監督受託者是否遵守規範。

（四）安全維護

此原則要求個資控管者採取合理而適當之安全維護措施以避免個資侵害事故的發生。

（五）個資完整性與目的限制

此原則要求個資控管者僅得於蒐集個資之目的內使用及保存當事人的個人資料，且個資控管者應採取合理步驟確保當事人個資的完整、正確與即時。

（六）當事人近用[3]

此原則要求個資控管者確保當事人得行使其更正、刪除個資等當事人權利。

（七）賠償、執行與責任

此原則要求個資當事人應獲得有效的賠償機制，以救濟其受侵害之權利；並且應有對違法者的有效處罰機制，以嚇阻其違法行為，以促使法律遵循。

[3] access 意義多元，各方中文翻譯亦不一致，本處譯為「近用」，其概念為「接近（取得）」或「使用」。

六、Schrems 案判決對我國的影響

歐盟法院的 Schrems 案判決旨在統一歐盟的法律解釋與適用，並對歐盟執委會的決定作出效力認定，未直接對我國有所影響。然而，該判決闡明第三國的個資保護程度適足性應有的內涵，值得我國政府作為借鏡。

據此，綜合本研究第貳章對歐盟第 29 條工作小組的 WP254 號文件之說明及本章所載歐盟 Schrems 案判決之分析，我國如為爭取通過歐盟執委會的個資保護程度適足性決定，除「法律（個人資料保護法）規範內容」應包含歐盟法律的基本概念或原則之外，尚應具備「有效促使法律遵循的監督與處罰機制」，以及「個資當事人能有效獲得救濟之機制」，簡述如下：

（一） 法律基本概念與原則

我國個人資料保護法乃參考歐盟個資保護指令及德、日等國個人資料保護法而訂，業將歐盟法律要求的諸如「正當性原則（個資法第 5 條）」、「目的限制原則（個資法第 16 條、第 20 條）、「個資品質與比例原則（個資法第 5 條、第 10 條、第 11 條、第 15 條、第 19 條等）、「個資保存原則（個資法第 11 條）、「安全與保密原則（個資法第 18 條、第 27 條）」、「透明

原則（個資法第 8 條、第 9 條）、「當事人權利保障原則（個資法第 3 條、第 10 條、第 11 條等）」納入法律規範。

惟就「（跨境傳輸後的）再傳輸限制原則」部分則未見規定；此外，2018 年 5 月 25 日生效的歐盟 GDPR 復對「當事人權利」之內容新增保障，強化個資當事人的「資訊自主權」，此權利內涵亦與我國法律存有落差。

（二） 促使法律遵循的監督與處罰機制

再就監督與處罰機制來看，我國目前於個資保護制度上仍未有「獨立」行使「調查與執法」權力之個資保護監管機關，恐將減損我國主張個資保護之適足程度；且 GDPR 加重個資控管者的法遵義務，設有諸多關於「個資治理（Data Governance）」之要求（例如資訊紀錄義務、個資保護官設置義務、預設個資保護義務、個資保護衝擊評估義務、事故通報監管機關義務、舉證合規義務等），均可強化歐盟組織的法律遵循程度，此等規範亦為訂定於我國個人資料保護法中。

此外，我國個人資料保護法對於違法機關的行政處罰罰鍰上限為新台幣 50 萬元，較以 GDPR 的罰鍰上限達 2000 萬歐元或該企業年度全球營收的 4%（取其高者），我國的處罰制度是否能有效嚇阻違法，確有待觀察。

（三） 個資當事人救濟機制

最後，依我國個人資料保護法規定，當涉及國家安全、刑事偵查、公共利益等因素時，蒐集個資機關（個資控管者）得在蒐集目的外利用個人資料，即可將保有之個人資料於原始目的外提供相關司法機關或行政機關（個資法第 16 條但書、第 20 條第 1 項但書參照），此例外規定將使個資當事人對其個人資料失去自主控管，且亦無管道（或權利）得知其個人資料是否遭司法機關或行政機關依前述目的取得，更遑論有效申訴以獲得救濟之機制。

即便可由司法程序請求法院客觀審查蒐集機關提供個資予司法機關或行政機關的合法性，但訴訟程序之時間、金錢等成本過高，是否能符合歐盟法律所謂「當事人能迅速、有效、低成本的獲得救濟以行使權利」的要求，不無疑問。

另由於我國個人資料保護法目前仍規定由各中央目的事業主管機關或直轄市、縣、市政府作為所轄事業或地區的個資保護主管機關，對於個資當事人的申訴事件能否有效受理、處置，並對當事人提供救濟，仍有賴具體資訊以彙整我國個資當事人獲得權利救濟的有效程度。

綜上所述，我國政府目前正處爭取通過歐盟執委會認定個資保護程度具備適足性之際，則對於前揭 WP254 號文件及歐盟法院於 Schrems 案的判決所述之評估因素，即應就我國法律規範內容及法遵監管制度與當事人救濟機制等面項審慎檢視其影響，如有修法需求更應盡速為之。

附件1：WP254 號文件中英文對照翻譯

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

[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。

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]。

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）。

[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。

[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。

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 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.

[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。

「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。

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。

[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。

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。

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].

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

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 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

[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。

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 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:

[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。

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

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

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

[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。

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

[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。

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 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 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)

[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。

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

附件2：歐盟法院 Schrems 案判決中英文對照翻譯

Judgment

判決

1 Judgment

判決

1 This request for a preliminary ruling relates to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter'), of Articles 25(6) and 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'), and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

本案請求先決判決[1]係關於歐盟基本權利憲章第 7、8、47 條（下稱憲章）、歐洲議會與歐盟理事會[2]於 1995 年 10 月 24 日個資處理與自由傳輸之個資保護會議（OJ 1995 L 281, p. 31）通過之歐盟第 95/46/EC 號指令第 25 條第 6 項及第 28 條，後經歐洲議會與歐盟理事會於 2003 年 9 月 29 日會議（OJ 2003 L 284, p. 1）修

[1] 譯注：preliminary ruling 係指歐盟會員國法院於訴訟中遇有涉及歐盟法律或條約之解釋爭議時，先暫停訴訟，並聲請 CJEU 做出先決判決，該先決判決為該歐盟法律之終局解釋，不僅拘束聲請解釋之法院，並拘束所有歐盟會員國法院，但該案件仍由聲請法院於接獲先決判決之解釋後，為最終判決

[2] 譯注：歐盟立法機關由歐盟理事會(Council of the EU 或稱為 Council of Ministers, 簡稱 the Council)與歐洲議會(European Parliament)所組成。其中歐盟理事會由成員國家部長級官員組成，相當於歐盟的上議院，歐洲議會則相當於歐盟的下議院。

正（No 1882/2003）之解釋，以及本質上關於執委會在 2000 年 7 月 26 日依據第 95/46 號指令針對安全港隱私原則保護適足性作成之決定（2000/520/EC），以及美國商務部發布之相關常見問答（OJ 2000 L 215, p. 7）之有效性。

2 The request has been made in proceedings between Mr. Schrems and the Data Protection Commissioner ('the Commissioner') concerning the latter's refusal to investigate a complaint made by Mr. Schrems regarding the fact that Facebook Ireland Ltd ('Facebook Ireland') transfers the personal data of its users to the United States of America and keeps it on servers located in that country.

本案係 Schrems 先生與資訊保護官（下稱保護官），針對該保護官駁回 Schrems 先生訴請調查臉書愛爾蘭有限公司（下稱臉書愛爾蘭）將用戶個人資料跨境傳輸至美國並保存於當地伺服器一案所提出。

Legal context

法規內容

Directive 95/46

95/46 指令

3 Recitals 2, 10, 56, 57, 60, 62 and 63 in the preamble to Directive 95/46 are worded as follows:

指令前言之說明第 2、10、56、57、60、62、63 點文字如下：

'(2) ... data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

…資料處理系統係為服務人群而設計…無論自然人之國籍或居住地，應尊重其基本權利與自由，尤以隱私權為最，並為個人福祉…帶來貢獻;

(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the

European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950,] and in the general principles of Community law; …, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

…國家個人資料處理相關法律之目的係保障基本權利與自由，特別是隱私權，已為歐洲人權與基本自由保護公約（1950 年 11 月 4 日於羅馬簽署）第 8 條與歐洲經濟共同體法一般法律原則所承認;…,因此，這些法律的相近部分，不可對其提供之保障造成減損，反而應在歐洲經濟共同體尋求更強度之保障;

(56) … cross-border flows of personal data are necessary to the expansion of international trade; … the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; … the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

… 個資跨境傳輸對國際貿易之拓展實屬必要;…. 歐洲經濟共同體藉由指令對個人之保障，並不妨礙將個人資料傳輸至具備個資保護適足程度之第三國;…而第三國之適足性保護程度，須就傳輸作業或一系列之傳輸作業所涉之所有情況加以評估;

(57) … on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

…另一方面，將個資傳輸至無法達到保護適足程度之第三國必須被禁止;

(60) … in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member

States pursuant to this Directive, and in particular Article 8 thereof;

…在任何情況下，只有在完全遵循會員國依據本指令（特別是第 8 條）通過之法規時，始能傳輸個人資料至第三國；

(62)… the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

…會員國設置完全獨立行使其權力之監管機關，係處理個資時對個人保護之必要條件;

(63)…such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...'

…該等監管機關必須具備必要之工具以行使職權，特別是對於個人提出之申訴，應具備包括調查及介入之權力，與參加訴訟程序之權力;…」

4 Articles 1, 2, 25, 26, 28 and 31 of Directive 95/46 provide:

95/46 指令第 1、2、25、26、28、31 條之內容：

'*Article 1* Object of the Directive

第 1 條 立法目的

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

依據本指令，會員國應保障自然人之基本權利與自由，特別是關於處理個資時之隱私權.

Article 2 Definitions

第 2 條 定義

For the purposes of this Directive:

本指令之目的：

(a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

「個人資料」係指任何有關識別或可得識別自然人（「個資當事人」）之任何資訊；可得識別之自然人係指得以直接或間接，特別是可藉由如身分識別號碼或一個或多個有關身體、生理、心理、經濟、文化或社會身分等具體因素加以識別。

(b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

「個人資料處理」（「處理」）係指任何對個人資料之操作或一系列操作，無論係透過自動化方式如蒐集、記錄、組織、儲存、改編或變更、檢索、參考、使用、傳輸揭露、傳播，或以其他方式使之得以利用、調整或組合、限制、刪除或銷毀。

(d) “controller” shall mean the natural or legal person, public authority, agency or any 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 processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

「控管者」係指單獨或與他人共同決定個資處理目的與方法之自然人或法人、公務機關、機構或其他任何主體；當處理個資之目的及方法係依會員國或歐洲經濟共同體之法律或規則決定時，控管者或其認定標準得由會員國法或歐洲經濟共同體法指定。

Article 25 Principles

第 25 條 原則

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

   會員國應規定，個資傳輸至第三國，無論是正在處理或傳輸後始處理，僅限於在不違反依本指令其他規定而訂定之會員國法規情形下，該第三國確保其具有適足的保護程度時，始得進行。

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

   第三國之資料保護適足性程度，應依據傳輸作業或一系列之傳輸作業所涉之所有可能情形加以評估，特別應考量資料之本質、可能之處理目的與處理期間、來源國與最終目的國、該第三國有效之一般及特別法規、專業規範與該國所採行之安全措施。

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

   會員國及執委會於認為第三國無法確保其符合第 2 項所述之適足保護程度時，應相互告知。

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this

Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

依第 31 條第 2 項所定程序，當執委會認定第三國無法確保其符合本條第 2 項所述之適足保護程度者，會員國應採取必要之措施，以防止同類資料傳輸至該第三國。

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

於適當時機，執委會應就第 4 項所導致之情事協商相關救濟事宜。

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

依第 31 條第 2 項規定，執委會得認定第三國基於其國內法或國際承諾（特別指第 5 項之協商結論），於私人生活及個人基本自由及權利之保護，具備第 2 項所述之適足保護程度。

Member States shall take the measures necessary to comply with the Commission's decision.

會員國應依據執委會之決定，採取必要措施。

Article 26 Derogations

第 26 條 例外規定

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

於不適用第 25 條及會員國之國內特別法之情況，會員國應規定傳輸或一系列傳輸資料至未能確保其符合第 25 條第 2 項所述適足保護程度之第三國之行為，於以下條件仍可進行：

(a) the data subject has given his consent unambiguously to the proposed transfer; or

個資當事人已明確同意該傳輸；或

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

該傳輸為履行個資當事人與控管者間契約之必要，或係為回應個資當事人之請求而履行契約成立前之相關措施；或

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

該傳輸係為控管者與第三人間締結或履行有利於個資當事人之契約所必須；或

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

該傳輸係基於維護重大公共利益所必需或合法要件，或為成立、執行或防禦法律上主張之必要;或

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

該傳輸係為保障個資當事人之重要利益之必要；或

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

該傳輸係登記機關於特殊情況下，為向不特定大眾或得主張合法利益之人徵詢意見，依據法定之徵詢條件，依法向大眾提供資料。

2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

於不違反第 1 項規定之情況下，當控管者提出對於個人隱私、基本權、自由之保護，以及可行使相關權利之適當安全維護時，會員國得許可進行單次或一系列之個資傳輸至未能確保其符合第 25 條第 2 項所述適足保護程度之第三國，此種安全維護得以適當之契約條款達成。

3. The Member State shall inform the Commission and the other Member States of the authorisations it grants pursuant to paragraph 2.

會員國應將其依第 2 項所為之許可通知執委會與其他會員國。

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31(2).

倘有會員國或執委會就個人隱私、基本權與自由保護以正當理由提出異議時，執委會應依第 31 條第 2 項規定之程序採取適當之措施。

Member States shall take the necessary measures to comply with the Commission’s decision.

會員國對於執委會之決定應採取必要措施予以遵循。

Article 28 Supervisory authority

第 28 條 監管機關

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

   各會員國應設立一個或多個公務機關，負責監管該國內依本指令訂定之法規適用情形。

   These authorities shall act with complete independence in exercising the functions entrusted to them.

   上開監管機關應獨立行使法定職權。

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

   各會員國應規定於研擬個人資料處理相關之權利與自由保護行政措施或法規時，須諮詢該等監管機關。

3. Each authority shall in particular be endowed with:

   各監管機關應特別被賦予以下權力：

   — investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

   — 調查權，例如取得與調查目標處理作業相關之資料，以及為行使其監督之責，蒐集所有相關必要資訊。

   — effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

— 有效介入權，例如在依第 20 條進行傳輸作業前表達意見，並確保該意見以適當方式公布；命令限制、刪除或銷毀資料；作成暫時性或永久性之資料傳輸禁令；警告或勸戒控管者；將相關事件提交國會或其他政治機構等。

— the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

— 針對違反依本指令訂定之國內法者，進行相關法律程序或移送司法機關之權力。

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

針對監管機關作成之決定，可上訴至法院。

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

   各監管機關應受理任何個人或其代理機構，就個資處理時相關權利與自由保護提出之申訴，且應通知當事人裁量結果。

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

當國內法依據本指令第 13 條訂定、適用時，各監管機關應就個資處理合法性的相關申訴特別注意，並至少應通知申訴人已進行該項確認。

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in

accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

各監管機關有權於該會員國領域內行使第 3 項賦予之權力，不論系爭處理行為應適用之國內法為何。各監管機關亦得依其他會員國監管機關之請求行使該權力。

Article 31

第 31 條

2. Where reference is made to this Article, Articles 4 and 7 of [Council] Decision 1999/468/EC [of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23)] shall apply, having regard to the provisions of Article 8 thereof.

對本條作成之解釋，考量第 8 條相關規定，應適用 1999/468/EC 決定之第 4 條及第 7 條（1999 年 6 月 28 日有關執委會執行權力之程序（OJ 1999 L 184, p. 23））。…」

Decision 2000/520

2000/520 決定

5 Decision 2000/520 was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

2000/520 決定係執委會依據 95/46 指令之第 25 條第 6 項而通過。

6 Recitals 2, 5 and 8 in the preamble to that decision are worded as follows:

該決定前言之說明第 2、5、8 點內容如下：

‘(2) The Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary.

「(2) 倘執委會認為某第三國確保具有適足保護程度，則會員國傳輸個資至該國無須額外必要之保障。

(5) The adequate level of protection for the transfer of data from the Community to the United States recognised by this

Decision, should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States (hereinafter "the Principles") and the frequently asked questions (hereinafter "the FAQs") providing guidance for the implementation of the Principles issued by the Government of the United States on 21 July 2000. Furthermore the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles implemented in accordance with the FAQs.

若組織遵循安全港隱私原則（下稱「安全港原則」）及美國政府 2000 年 7 月 21 日就如何實施安全港原則所發布之常見問題（下稱「常見問答」），以保障由會員國傳輸至美國之個資，則本決定確認由歐盟傳輸個資至美國具備適足保護程度。此外，各組織應公開揭露隱私政策，並依聯邦貿易委員會法第 5 條有關禁止不公平或詐欺之商業行為或影響商業之行為規定，由聯邦貿易委員會（FTC），或其他可有效確保依據常見問答履行安全港原則之法定組織管轄。

(8) In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.'

基於透明度，並維護會員國主管機關確保個人資料受到保護之能力，應在本決定中列出適足保護程度下之例外情形，排除特定之資料傳輸。

7 Articles 1 to 4 of Decision 2000/520 provide:

2000/520 決定第 1 條至第 4 條規定：

‘*Article 1*

「*第 1 條*

1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the “Safe Harbour Privacy Principles” (hereinafter “the Principles”), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter “the FAQs”) issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

   為 95/46/EC 指令第 25 條第 2 項之目的，所有屬該指令範圍之行為，如依本決定附件 2 美國商務部 2000 年 7 月 21 日發布之常見問題（即常見問答）履行本決定附件 1 安全港隱私原則（即安全港原則），並考量下列美國商務部發布之文件，則自歐洲經濟共同體傳輸個資至設立於美國之組織，應認為具備適足保護程度：

   (a) the safe harbour enforcement overview set out in Annex III;

   附件 3 之安全港執行概要。

   (b) a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;

   附件 4 之違反美國法明確授權及隱私規定之損害賠償備忘錄。

   (c) a letter from the Federal Trade Commission set out in Annex V;

   附件 5 之聯邦貿易委員會函。

   (d) a letter from the US Department of Transportation set out in Annex VI.

   附件 6 之美國交通部函。

2. In relation to each transfer of data the following conditions shall be met:

任何個資傳輸均應符合下列條件：

(a) the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

接收個資之組織應明確且公開的揭示承諾，願意遵循依據常見問答履行之安全港原則；

(b) the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

該組織應受本決定附錄 VII 所列之美國政府機關(構)管轄，不論該個人之國籍或居住地為何，凡未遵循常見問答履行安全港原則，機關均有權調查申訴事件、對個人所遭受之不公平或詐欺行為提供救濟與糾正。

3. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

各該自我證明其依照常見問答履行安全港原則之組織，自通知美國商務部(或其指定者)依第 2 項 a 款公開揭露之承諾，及其受管轄之政府機關(構)（第 2 項 b 款所列）起，即應認為該組織已符合第 2 項所訂條件。

Article 2

第 2 條

This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States, in particular Article 4 thereof.

本決定僅針對美國依據常見問題履行安全港原則之保護適足性，以期符合 95/46/EC 指令第 25 條第 1 項之要求，並不影響該指令之其他條款於會員國內處理個資之適用，特別是第 4 條。

Article 3

第 3 條

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:

於不損及會員國主管機關（構）確保依 95/46/EC 指令第 25 條以外規定所訂定之國內法之執行，會員國主管機關（構）得於下列情形，行使現行職權對於已自我證明其依常見問答履行安全港原則之組織，暫停其個資傳輸，以保障個人資料之處理：

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

經本決定附件 7 所列之美國政府機關（構）或附件 1 之執行原則(a)之獨立協助機制，認定該組織違反依常見問答履行之安全港原則；或

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

有重大可能性將違反安全港原則；合理確信該執行機制未採取或將不會採取適當與即時的措施解決系爭個案；持續的傳輸可能會對個資當事人造成重大損害之立即風險；且會員國之主管機關在該情境下已作出合理之努力，通知該組織並給予回應機會。

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

只要確認已遵循依常見問答履行之安全港原則，並通知歐洲經濟共同體之主管機關，傳輸中止之禁令應儘速廢止，。

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

會員國依據第 1 款採行相關措施時，應立刻通知執委會。

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States fails to secure such compliance.

會員國與執委會應就美國境內組織無法確保依常見問答實施安全港原則之行為，互相通報。

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that anybody responsible for ensuring compliance with the Principles implemented in accordance with the FAQs in the United States is not effectively fulfilling its role, the Commission shall inform the US Department of Commerce and, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC with a view to reversing or suspending the present Decision or limiting its scope.

倘依第 1、2、3 款蒐集之資訊證明任何負責確保依常見問答有效遵循安全港原則之組織無法有效擔任其角色時，執委會應通知美國商務部，必要時得依第 95/46/EC 號指令第 31 條提出因應措施建議，以推翻或中止現行決定或限制其適用範圍。

Article 4

第 4 條

1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.

本決定可隨時依安全港原則之執行狀況，及/或美國法律規範已納入安全港原則及常見問答之保護程度時，進行修正。

The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.

無論如何，執委會對會員國作出通知 3 年後，應以可得資訊為基礎，評估現行決定之執行狀況，並將相關發現提報依 95/46/EC 指令第 31 條設立之委員會，包括任何可能影響依本決定第 1 條

規定提供符合 95/46/EC 指令第 25 條定義之適足保護程度法規之評估之證據，以及任何關於現行決定被差異執行之證據。

2.The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.'

執委會應在必要之時依 95/46/EC 指令第 31 條規定之程序提出因應措施建議。」

8 Annex I to Decision 2000/520 is worded as follows:

2000/520 決定附錄 I 內容如下：

'Safe Harbour Privacy Principles'

「安全港隱私原則」

issued by the US Department of Commerce on 21 July 2000

美國商務部 2000 年 7 月 21 日發布

... the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. …

…為培育、促進與發展國際商務，美國商務部基於法定職權發布此份文件與常見問題（安全港原則）。本原則係諮詢產業界與公眾意見而制定，俾利促進美國與歐盟間之貿易與商務。本原則僅供接收歐盟個資之美國組織，為取得符合安全港規範與可能產生之個資保護「適足性」資格之用。茲因安全港原則僅為上開特定目的而制定，不宜為其他目的適用。

Decisions by organisations to qualify for the safe harbour are entirely voluntary, and organisations may qualify for the safe harbour in different ways. ...

各組織可自行決定是否取得安全港資格，且資格取得方式亦可不同。

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation; or (c) if the effect of the Directive [or] Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organisations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or US law, organisations are expected to opt for the higher protection where possible.

此等原則之遵循得受下列情況限制：(a)為符合國家安全、公共利益或執法要求所必須；(b)組織可舉證其因法律、政府法規或判例法所產生之義務衝突，或因執行明確之授權及此種授權產生之優位合法利益所必須，故未遵循安全港原則；(c)本指令之法律效果或會員國法如允許例外或排除情形，且此例外或排除適用之背景相似。配合強化隱私保護目的，組織應積極充分且透明地實施安全港原則，包括定期在渠等隱私政策中標明，符合上開(b)條件而適用安全港原則之例外情況。同理，在安全港原則及/或美國法允許自由選擇之狀況下，期盼組織盡可能選擇提供更高標準的個資保護。

9 Annex II to Decision 2000/520 reads as follows：Frequently Asked Questions (FAQs)

附件II2000/520決定如下：常見問題(FAQs)

(1)FAQ 6 — Self-Certification

(1)常見問答6─自我證明

Q: How does an organisation self-certify that it adheres to the Safe Harbour Principles?

組織如何自我證明其符合安全港原則？

A: Safe harbour benefits are assured from the date on which an organisation self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

組織自向商務部(或其指定者)提出自我證明，其已根據下列指引遵循安全港原則之日起，即得享有安全港之利益。

To self-certify for the safe harbour, organisations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organisation that is joining the safe harbour, that contains at least the following information:

為自我證明符合安全港原則，參與安全港原則之組織得向商務部(或其指定者)提交一封由公司管理階層以公司名義簽署之文件，該文件至少應包含下列資訊：

1. name of organisation, mailing address, e-mail address, telephone and fax numbers;

組織之名稱、通訊地址、電子郵件地址、電話和傳真號碼；

2. description of the activities of the organisation with respect to personal information received from the [European Union]; and

說明組織中關於「歐盟」來源個資之相關業務;及

3. description of the organisation's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requests, and any other issues arising under the safe harbour, (d) the specific statutory body that has jurisdiction to hear any claims against the organisation regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programmes in which the organisation is a member, (f) method of verification (e.g. in-house, third party) …, and (g) the independent recourse mechanism that is available to investigate unresolved complaints.

   說明，包含：(a) 大眾可得查閱隱私政策之處，(b) 該隱私政策的生效日期，(c) 處理申訴、查詢和其他關於安全港議題之聯絡辦公室，(d) 具有管轄權處理該組織不公平或詐欺，與違反隱私法規（如安全港原則附件所列行為）之申訴之特定法定機構，(e) 任何該組織以會員身份參加之隱私計畫名稱，(f) 認證方式（如公司自我宣稱、第三公正單位認證），(g)調查未決申訴之獨立協助機制。

Where the organisation wishes its safe harbour benefits to cover human resources information transferred from the [European Union] for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organisation arising out of human resources information that is listed in the annex to the Principles. ...

組織如希望其安全港效益涵蓋雇傭關係中來自「歐盟」之人資資料，只要如安全港原則附件所列，具備有司法審理權之法定機構，即可審理因人資資料所引起之申訴。...

The Department (or its designee) will maintain a list of all organisations that file such letters, thereby assuring the availability of safe harbour benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11. ...

商務部（或其指定者）將建置提交此類文件之組織名單，以確保安全港效益，並依據常見問答11提交之年度申請文件及通知更新該名單。

FAQ 11 — Dispute Resolution and Enforcement

常見問答11─紛爭解決與執行

Q: How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organisation's persistent failure to comply with the Principles be handled?

如何落實執行原則所定之紛爭解決要件？如何處理持續不遵循安全港原則之組織？

A: The Enforcement Principle sets out the requirements for safe harbour enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organisations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programmes that incorporate the Safe Harbour Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities

located in the European Union or their authorised representatives. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirements set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

執行原則臚列安全港原則之執行要件。如何符合該原則要點（b)之要件係載明於常見問答有關驗證部分(常見問答7)。常見問答11說明要點（a）與（c），兩者皆要求獨立之協助機制。機制樣態可相異，惟均須符合執行原則之要件。組織可透過以下的方式，符合相關規定：(1) 遵循私部門的隱私計畫，將安全港原則納入其規則，並包含執行原則所述之有效執行機制；(2) 遵循法律或提供個人申訴處理和紛爭解決之監管機關；或(3) 承諾與歐盟境內之資料保護機構或其授權機構合作。

以上各項僅係舉例說明而非限制。私部門得設計其他執行機制，只要該機制符合執行原則和常見問答之要件。須注意者為，執行原則之要件係安全港原則前言第3段之補充規定，依據聯邦貿易委員會法第5條或類似法規，自律機制必須具有可執行性。

Recourse Mechanisms

協助機制

Consumers should be encouraged to raise any complaints they may have with the relevant organisation before proceeding to independent recourse mechanisms. ...

在依獨立協助機制提出申訴之前，應鼓勵消費者先向相關組織投訴。...

FTC Action

聯邦貿易委員會(FTC) 行為

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organisations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbour Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. ...

聯邦貿易委員會承諾，優先審查隱私自律組織(如BBBOnline與TRUSTe)所提出案件，及歐盟會員國指控不遵守安全港原則之案件，以確認是否違反聯邦貿易委員會法第5節禁止從事不公平或詐欺之商業活動。…

10 Annex IV to Decision 2000/520 states:

2000/520號決定之附件IV提到：

‘Damages for Breaches of Privacy, Legal Authorisations and Mergers and Takeovers in US Law

「美國法律關於違反隱私權、法律授權及公司合併與收購之損害賠償」

This responds to the request by the European Commission for clarification of US law with respect to (a) claims for damages for breaches of privacy, (b) “explicit authorisations” in US law for the use of personal information in a manner inconsistent with the safe harbour principles, and (c) the effect of mergers and takeovers on obligations undertaken pursuant to the safe harbour principles.

此係回應歐盟執委員會以澄清美國法律有關以下事項（a）隱私權受侵害之損害求償權，（b） 美國法律中關於「明確授權」使用個人資料之方式不符安全港原則，以及(c)依安全港原則所負義務，對公司合併與收購之影響。

B. Explicit Legal Authorisations

明確法律授權

The safe harbour principles contain an exception where statute, regulation or case-law create "conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorisation". Clearly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law. As for explicit authorisations, while the safe harbour principles are intended to bridge the differences between the US and European regimes for privacy protection, we owe deference to the legislative prerogatives of our elected lawmakers. The limited exception from strict adherence to the safe harbour principles seeks to strike a balance to accommodate the legitimate interests on each side.

安全港原則包含一個例外，即法律、法規或判例法產生「義務衝突或明確授權時，若組織可證明其執行任何此類授權而違反安全港原則，係以符合該授權所生之優位合法利益之範圍為限」。顯然，美國法律加諸之衝突義務，無論美國組織是否在安全港適用範圍內皆必須遵守其法律。至於明確授權，雖然安全港原則係為橋接美國和歐洲隱私保護制度之差異，但我們仍必須尊重立法者之立法特權。嚴格遵守安全港原則之有限例外規定，係尋求調和雙方合法利益之平衡點。

The exception is limited to cases where there is an explicit authorisation. Therefore, as a threshold matter, the relevant statute, regulation or court decision must affirmatively authorise the particular conduct by safe harbour organisations ... In other words, the exception would not apply where the law is silent. In addition, the exception would apply only if the explicit authorisation conflicts with adherence to the safe harbour principles. Even then, the exception "is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation". By way of illustration, where the law simply authorises a company to provide personal

information to government authorities, the exception would not apply. Conversely, where the law specifically authorises the company to provide personal information to government agencies without the individual's consent, this would constitute an "explicit authorisation" to act in a manner that conflicts with the safe harbour principles. Alternatively, specific exceptions from affirmative requirements to provide notice and consent would fall within the exception (since it would be the equivalent of a specific authorisation to disclose the information without notice and consent). For example, a statute which authorises doctors to provide their patients' medical records to health officials without the patients' prior consent might permit an exception from the notice and choice principles. This authorisation would not permit a doctor to provide the same medical records to health maintenance organisations or commercial pharmaceutical research laboratories, which would be beyond the scope of the purposes authorised by the law and therefore beyond the scope of the exception ... The legal authority in question can be a "stand alone" authorisation to do specific things with personal information, but, as the examples below illustrate, it is likely to be an exception to a broader law which proscribes the collection, use, or disclosure of personal information.

安全港原則之例外僅限於有明確授權之情形。因此，以此為門檻，相關的法律、規定或法院裁判必須明確授權安全港組織之特定行為...換言之，當法律未規定時，此一例外情形即不適用。此外，例外情形僅限於明確授權與符合安全港原則相衝突時始適用。即便此一例外情形係「僅限於為達到重大合法利益之必要範圍內」。舉例言之，如果法律僅授權一家公司提供個資給政府機構，即不適用此例外規定。相反地，如果法律特別授權公司在未取得個人同意之情況下，可提供其個資給政府機構，即屬與安全港原則相衝突之「明確授權」。另外，提供通知和同意之特定情況，亦屬於例外情況（係相當於在未通知及取得同意的情況下揭露資訊之特定授權）。例如，法律授權醫生在未得患者之事先同意下，向衛生機構提供患者的醫療紀錄，應屬允許通知與選擇原則之例外

情形。此一授權並不允許醫生向健康維護組織或商業藥物研究實驗室提供同樣的醫療紀錄，如此一來，即會超出法律授權之範圍，亦超出例外情形之範圍。...系爭法律主管機關可能「獨立」授權使用個資做特定事情，但正如以下例子所示，它有可能是禁止蒐集、使用或揭露個人資料等更廣泛法律之例外。

Communication COM(2013) 846 final

歐盟執委會政策文件 COM(2013) 846 最終版

11 On 27 November 2013 the Commission adopted the communication to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) ('Communication COM(2013) 846 final'). The communication was accompanied by the 'Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection', also dated 27 November 2013. That report was drawn up, as stated in point 1 thereof, in cooperation with the United States after the existence in that country of a number of surveillance programmes involving the large-scale collection and processing of personal data had been revealed. The report contained inter alia a detailed analysis of United States law as regards, in particular, the legal bases authorising the existence of surveillance programmes and the collection and processing of personal data by United States authorities.

2013 年 11 月 27 日，歐盟執委會通過了送交歐洲議會和歐盟理事會的政策文件「重建歐洲與美國資料流動之信任」（COM（2013）846 final）（'Communication COM（2013）846 final'）。該案附有 2013 年 11 月 27 日歐盟與美國資料保護工作小組歐盟聯合主席的調查結果報告。誠如報告第 1 點所述，該報告係在美國大規模蒐集和處理個人資料的監控計畫被揭露之後，與美國合作撰寫完成。該報告內容包括美國法律之詳細分析，特別是現存監控計畫以及美國政府蒐集和處理個人資料之法源依據。

12 In point 1 of Communication COM(2013) 846 final, the Commission stated that '[c]ommercial exchanges are addressed by Decision

[2000/520]', adding that '[t]his Decision provides a legal basis for transfers of personal data from the [European Union] to companies established in the [United States] which have adhered to the Safe Harbour Privacy Principles'. In addition, the Commission underlined in point 1 the increasing relevance of personal data flows, owing in particular to the development of the digital economy which has indeed 'led to exponential growth in the quantity, quality, diversity and nature of data processing activities'.

執委會於「重建歐洲與美國資料流動之信任」文件(Communication COM(2013) 846 final）第 1 點指出，商業交流議題已於 2000/520 決定處理，針對自歐盟傳送個資至美國境內符合安全港隱私原則的公司，該決定提供了法律基礎。此外，執委會在第 1 點強調個人資料流動日益重要，特別是因為數位經濟的發展，導致資料處理活動在數量、質量、多樣性和性質上呈現指數型成長。

13 In point 2 of that communication, the Commission observed that 'concerns about the level of protection of personal data of [Union] citizens transferred to the [United States] under the Safe Harbour scheme have grown' and that '[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement'.

執委會在該文件第 2 點指出，其對依安全港協議傳送歐洲公民個資至美國的保護程度的關切度提高，且由於該協議之自願性和宣示性，已將重點集中於協議之透明度與執行面。

14 It further stated in point 2 that '[t]he personal data of [Union] citizens sent to the [United States] under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the [European Union] and the purposes for which it was transferred to the [United States]' and that '[a] majority of the US internet companies that appear to be more directly concerned by [the surveillance] programmes are certified under the Safe Harbour scheme'.

該文件第 2 點進一步在指出，依據安全港協議，傳送至美國的歐洲公民個資，可能會被美國政府以不符合該資料 (自歐盟)蒐集之原始目的，或該資料傳輸至(美國)之目的而取得並進一步處理。且多數美國與監控計畫直接相關之網路公司，已依安全港協議獲得認證。

15 In point 3.2 of Communication COM(2013) 846 final, the Commission noted a number of weaknesses in the application of Decision 2000/520. It stated, first, that some certified United States companies did not comply with the principles referred to in Article 1(1) of Decision 2000/520 ('the safe harbour principles') and that improvements had to be made to that decision regarding 'structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception'. It observed, secondly, that 'Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the [European Union] to the [United States] by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes'.

在該文件的第 3.2 點，執委會提及 2000/520 決定在適用上之數個缺點。首先，文件指出部分經安全港認證的美國公司並未遵守 2000/520 決定第 1 條第 1 項規定之原則（即「安全港原則」），必須改善該決定中關於「透明度和執行有關的結構性缺陷，安全港實質原則和國家安全運作之例外規定。其次，該文件亦指出，美國公司須依美國情報收集計劃提供美國情報機構資料，安全港協議因而亦成為其將歐洲公民個資自歐盟傳輸至美國之管道。

16 The Commission concluded in point 3.2 that whilst, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would[, however,] adversely affect the interests of member companies in the [European Union] and in the [United States]'. Finally, the Commission added in that point that it would 'engage with the US authorities to discuss the shortcomings identified'.

執委會在第 3.2 點總結，基於上述缺點，安全港目前之執行方式不能被維持，但廢止安全港卻可能對在歐盟和美國之會員公司產生不利的影響。最後，執委會補充，將會與美國政府討論這些缺點。

Communication COM(2013) 847 final

政策文件 COM(2013) 847 最終版

17 On the same date, 27 November 2013, the Commission adopted the communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the [European Union] (COM(2013) 847 final) ('Communication COM(2013) 847 final'). As is clear from point 1 thereof, that communication was based inter alia on information received in the ad hoc EU-US Working Group and followed two Commission assessment reports published in 2002 and 2004 respectively.

同日，2013 年 11 月 27 日，歐盟執委會通過了提交歐洲議會和歐盟理事會之從歐洲公民和企業觀點論安全港協議運作之政策文件(COM(2013) 847 final) ('政策文件 COM(2013) 847 final')。如該文件第 1 點所述，該文件除依據歐盟─美國工作小組之資訊，亦含括執委會 2002 年、2004 年所發表的兩份評估報告。

18 Point 1 of Communication COM(2013) 847 final explains that the functioning of Decision 2000/520 'relies on commitments and self-certification of adhering companies', adding that '[s]igning up to these arrangements is voluntary, but the rules are binding for those who sign up'.

政策文件(COM(2013) 847 final)第 1 點說明，2000/520 決定之運作「有賴同意遵循該原則公司之承諾和自我證明」，同時，「簽署係屬自願性質，但法規對簽署者具拘束力」。

19 In addition, it is apparent from point 2.2 of Communication COM(2013) 847 final that, as at 26 September 2013, 3246

companies, falling within many industry and services sectors, were certified. Those companies mainly provided services in the EU internal market, in particular in the internet sector, and some of them were EU companies which had subsidiaries in the United States. Some of those companies processed the data of their employees in Europe which was transferred to the United States for human resource purposes.

同時，該文件(COM(2013) 847 final)第 2.2 點指出，截至 2013 年 9 月 26 日，已有 3246 家產業或服務業部門公司（許多）獲得認證。這些公司主要係提供歐盟內部市場服務，尤其是網路業。其中部分公司是歐盟公司並在美國有分公司，基於人資管理需要，將歐盟境內員工資料處理後傳輸至美國。

20 The Commission stated in point 2.2 that '[a]ny gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme'.

執委會於該文件第 2.2 點指出，安全港因美方透明度或執行上之落差，導致責任轉移至歐盟資料保護機構與使用該協議之公司。

21 It is apparent, in particular, from points 3 to 5 and 8 of Communication COM(2013) 847 final that, in practice, a significant number of certified companies did not comply, or did not comply fully, with the safe harbour principles.

特別是依該文件(COM(2013) 847 final)第 3 點到第 5 點及第 8 點所述，實務上，許多經認證之公司並未遵循或未完全遵循安全港原則。

22 In addition, the Commission stated in point 7 of Communication COM(2013) 847 final that 'all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to US authorities to data stored and processed in the [United States], appear to be Safe Harbour certified' and that '[t]his has made the Safe Harbour scheme one of the conduits

through which access is given to US intelligence authorities to collecting personal data initially processed in the [European Union]'. In that regard, the Commission noted in point 7.1 of that communication that 'a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed [by] companies based in the [United States]' and that '[t]he large-scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in [Decision 2000/520]'.

再者，執委會於該文件第 7 點指出，所有涉及稜鏡計畫（PRISM programme）（一個大規模的情報蒐集計畫）的公司，顯示皆獲安全港認證；稜鏡計畫使美國政府得取得在美國儲存和處理之資料，而安全港協議則成為美國情報機構蒐集歐盟個資的管道之一。在這方面，執委會續於該文件第 7.1 點指出，美國法有多處法源依據允許設立於美國之公司得大規模儲存或處理個資，而這些監控計畫之大規模特質，可能導致美國政府在未符第 2000/520 號決定之例外要件，即為維護國家安全之絕對必要與比例原則情況下，取得依安全港協議傳輸之個資並再予處理。

23 In point 7.2 of Communication COM(2013) 847 final, headed 'Limitations and redress possibilities', the Commission noted that 'safeguards that are provided under US law are mostly available to US citizens or legal residents' and that, '[m]oreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes'.

執委會於該文件第 7.2 點「限制和救濟可能性」，強調，美國法規定之保護措施大多僅適用於美國公民或合法居民。此外，針對美國監控計畫下被蒐集及處理之個資，歐盟或美國個資當事人均無從申請使用、更正或刪除，亦無行政或司法救濟之可能。

24 According to point 8 of Communication COM(2013) 847 final, the certified companies included '[w]eb companies such as Google, Facebook, Microsoft, Apple, Yahoo', which had 'hundreds of millions of clients in Europe' and transferred personal data to the United States for processing.

依該文件第 8 點，經安全港認證的公司包含谷歌、臉書、微軟、蘋果及雅虎，這些公司在歐洲皆擁有數億名客戶，且均已將客戶個資傳輸至美國處理。

25 The Commission concluded in point 8 that 'the large-scale access by intelligence agencies to data transferred to the [United States] by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the [United States]'.

執委會於該文件第 8 點總結，「情報機構大規模取得經安全港認證公司傳輸至美國之資料，帶來額外嚴重的問題，亦即歐洲人個資被傳輸至美國時，其個資保護權利是否能持續。

The dispute in the main proceedings and the questions referred for a preliminary ruling

主程序爭議及提請先決判決之問題

26 Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

Schrems 先生係住在奧地利之奧地利籍人士，他自 2008 年起成為臉書網路社群臉書(「臉書」)之用戶。

27 Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located

in the United States, where it undergoes processing.

任何欲使用臉書的歐盟居民，須在其註冊時，與臉書愛爾蘭分公司簽約，而該公司總部係設於美國。歐盟境內愛爾蘭臉書分公司用戶的部分或全部個資，皆經傳輸至位於美國臉書總公司之伺服器進行處理。

28 On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

Schrems 先生於 2013 年 6 月 25 日向資訊保護官申訴，要求其行使法定權力禁止愛爾蘭臉書公司傳輸其個資至美國。Schrems 先生主張美國法律與實務，無法確保領域內個資具適足保護程度以防止政府監控行為。Schrems 先生於此提及愛德華·史諾登(Edward Snowden)所揭露之美國監控機構活動，尤其是美國國家安全局('the NSA')。

29 Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States

ensured an adequate level of protection.

由於該資訊保護官認為無義務調查 Schrems 先生申訴案之事實，遂以該案無事實根據駁回該請求。該資訊保護官認為並無事證顯示 Schrems 先生之個資已為美國國家安全局(NSA)取得。他並說明，基於美國個資保護適足性之問題須依 2000/520 決定判斷，且歐盟執委會已確認美方對個資保護已具適足保護程度，因此 Schrems 先生之申訴無法繼續進行。

30 Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

Schrems 先生向高等法院提起訴訟，並於主程序爭執該保護官之決定。高等法院考慮了訴訟當事人在主要訴訟程序所提出之證據後，發現對歐盟傳送至美國的個資所為之電子監控或截取行為，符合公共利益之必要性與不可或缺性。然而，高等法院亦指出由愛德華·史諾登所揭露之事實顯示，美國國家安全局及其他聯邦機構所為「顯著地超出其應有職權範圍」。

31 According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and carried out by them on a large scale.

高等法院指出，歐洲公民並無有效之意見陳述權。監控機構行為

之監督係於單方面之祕密程序之架構下進行。一旦個資被傳送至美國，即有可能被國家安全局，或聯邦調查局(FBI)等美國聯邦機構在大規模的全面監控過程中使用。

32 The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

高等法院表示，愛爾蘭法律規範，除第三國確保對人民隱私及基本權利自由具有適足程度之保護外，禁止將個資傳輸至其領域之外。愛爾蘭憲法保障隱私權及住宅不可侵犯權之重要性，要求這些權利之妨礙須符合法律規定與比例原則。

33 The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

高等法院亦指出，大量無差異地取得個資，明顯違反比例原則及

愛爾蘭憲法所保障之基本價值。電子傳輸個資截取行為，須證明其資料擷取係針對特定目標，其對某人或某團體之監控符合國家安全利益或抑制犯罪目的之客觀合理性，以及具備適當且可供查證之保護措施之要件，始符合愛爾蘭憲法規定。因此，高等法院表示，如果僅依愛爾蘭法律處理主程序，基於對美國是否確保具個資適足保護程度之嚴重懷疑，保護官應調查 Schrems 先生申訴案提出之問題，保護官乃不當駁回 Schrems 先生之申訴。

34 However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

然而，高等法院認為此一案件涉及在憲章第 51 條規定下歐盟法的實施，即該主程序爭議裁決之合法性須依歐盟法進行評估。高等法院指出，第 2000/520 號決定不符合憲章第 7 條和第 8 條，及歐盟法院在數位權利愛爾蘭 (Digital Rights Ireland and Others)(C-293/12 及 C-594/12, EU:C:2014:238) 乙案中所建立之原則。政府機關如於無保障國家安全或預防犯罪之客觀理由，亦無適當可供查證的保護措施配套，即隨意或普遍被授權取得電子通訊，則憲章第 7 條所保障且為各會員國共同傳統核心價值之隱

私尊重權，將不具意義。

35 The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

高等法院進一步認為，Schrems 先生所提之訴訟，實際上涉及建立安全港協議之第 2000/520 號決定之合法性，此亦為主程序中引發爭議之決定。 Schrems 先生即使形式上未對第 95/46 號指令或第 2000/520 號決定之有效性提出質疑，高等法院認為，問題在於依據第 95/46 號指令第 25 條第 6 項規定，保護官是否受執委會第 2000/520 號決定有關美國確保具適足保護程度之認定所拘束，或依憲章第 8 條規定授權保護官如認為適當則可不受上述認定之拘束。

36 In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary

contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

在這些情形下，高等法院決定停止訴訟程序，並將下列問題提交給歐洲法院為先決判決：

(1) 獨立個資保護官依法對被傳輸至第三國之個資（於本案，第三國係指美國），行使個資保護管理與執法權，而當該國法律及實務遭訴對個資當事人缺乏適足保護時，該個資保護官是否須受依憲章第7條、第8條和第47條，及第95/46號指令第25條第6項規定通過之第2000/520號決定所包含之歐洲經濟共同體的認定所拘束，儘管該認定與個資當事人之主張相左？

(2) 或者，自執委會的決定首度公告後，該個資保護官是否得或須依事實發展自行調查？

Consideration of the questions referred

提請解釋問題之考量

37 By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data

relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

統整所詢問題，提請解釋之法院本質上希望了解根據憲章第 7 條、第 8 條和第 47 條解讀第 95/46 號指令第 25 條第 6 項規定，是否以及在何種程度上，根據前開規定所通過之決定，例如第 2000/520 號決定，執委會於該決定認為第三國已確保指令第 28 條之適足程度保護，使會員國監管機關無從審查某人有關於處理其個人資料時之權利和自由，該處理係指資料從會員國傳送至第三國，且該民眾聲稱第三國實施的法律並無法確保適足程度的保護。

The powers of the national supervisory authorities, within the meaning of Article 28 of Directive 95/46, when the Commission has adopted a decision pursuant to Article 25(6) of that directive

當執委會依第 95/46 號指令第 25 條第 6 項通過決定之情況下，國家監管機關依該指令第 28 條所具有之權力

38 It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter (see judgments in *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68; *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 68; and *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 29).

首先，因第 95/46 號指令之條款係為管理可能侵犯基本自由（特別是尊重私人生活之權利）之個資處理行為，因此必須依據憲章所保障之基本權解釋 (請參照判決 *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 及 C-139/01, EU:C:2003:294, 第 68 段; *Google Spain and Google*, C-131/12, EU:C:2014:317, 第 68 段; 及

Ryneš, C-212/13, EU:C:2014:2428,第 29 段) 。

39 It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case-law of the Court (see judgments in *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 47; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 53; and *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs, 53, 66, 74 and the case-law cited).

第 95/46 號指令第 1 條及前言第 2 點至第 10 點明確指出，該指令不只是為確保自然人基本權利與自由之有效及完整保護，特別是個人資料處理中尊重私生活權利之保護，亦高度保護這些基本權利與自由。憲章第 7 條所保障之尊重私生活基本權，及憲章第 8 條所保障之個人資料保護基本權的重要性，也在下列案例中被強調 (請參照判決 *Rijkeboer*, C-553/07, EU:C:2009:293, 第 47 段; *Digital Rights Ireland and Others*, C-293/12 及 C-594/12, EU:C:2014:238, 第 53 段;及 *Google Spain and Google*, C-131/12, EU:C:2014:317, 第 53, 66, 74 段及引用之判例法) 。

40 As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary

law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in *Commission* v *Austria*, C-614/10, EU:C:2012:631, paragraph 36, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 47).

關於國家監管機關在傳輸資料至第三國方面之權力，值得注意的是，第 95/46 號指令第 28 條第 1 項要求會員國須設立一個或多個完全獨立之公務機關負責監管符合歐盟對於處理個人資料保護之規定。此外，此一要求係源自於歐盟之主要法律，特別是憲章第 8 條第 3 項及歐盟運作條約（TFEU）第 16 條第 2 項（請參照判決 *Commission* v *Austria*, C-614/10, EU:C:2012:631, 第 36 段,及 *Commission* v *Hungary*, C-288/12, EU:C:2014:237, 第 47 段）。

41 The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 25, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

國家監管機關獨立性之保障，係為確保監督個人資料保護法規合規性之效能與可靠度。該機關之設立係為加強受各機關決定影響之個人及機構之保護。因此，第 95/46 號指令前言第 62 點指出，會員國設立獨立監管機關係屬保護個人資料處理之重要環節(請參照判決 *Commission* v *Germany*, C-518/07, EU:C:2010:125 第 25 段及 *Commission* v *Hungary*, C-288/12, EU:C:2014:237 第 48 段及

引用之判例法)。

42 In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in *Commission* v *Germany*, C-518/07, EU:C:2010:125, paragraph 24, and *Commission* v *Hungary*, C-288/12, EU:C:2014:237, paragraph 51).

為確保此一保護措施，國家監管機關尤其應確保隱私基本權及個人資料自由流動之利益，其兩者間之平衡(請參照判決 *Commission* v *Germany*, C-518/07, EU:C:2010:125 第 24 段及 *Commission* v *Hungary*, C-288/12, EU:C:2014:237, 第 51 段)。

43 The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

為達此一目的，國家監管機關擁有廣泛的權力。這些權力在第 95/46 號指令第 28 條第 3 項規定並未詳盡列出，該指令前言第 63 點指出這些權力構成該機關履行職責之必要工具，因此，這些機關擁有調查權，即為履行該監督職責有權蒐集所有資訊，又或者是具有效介入之權力，即對個人資料處理施以暫時或明確禁制令，或有權進行訴訟。

44 It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of

Article 28 in respect of processing of such data carried out in a third country.

從第 95/46 號指令第 28 條第 1 項和第 6 項中可以明顯看出，國家監管機關的權力僅限於其會員國領土內所進行的個人資料處理，因此依據第 28 條的規定，國家監管機關對在第三國進行之資料處理並無監管之權力。

45 However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in *Parliament* v *Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'.

然而，將個人資料從會員國傳輸至第三國的行為，即構成了第 95/46 號指令第 2 條第 b 款所指的個人資料處理（請參考判決 *Parliament* v *Council and Commission*, C-317/04 及 C-318/04, EU:C:2006:346, 第 56 段）。該條文定義「個人資料處理」為對個人資料進行任何操作或一連串操作，不論是否以自動化方式為之，舉例來說，藉由傳送、散播或其他方式加以揭露。

46 Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect,

judgment in *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 63).

第 95/46 號指令前言第 60 點指出，只有在完全符合會員國依該指令通過之規定，才能將個人資料傳輸至第三國。在這方面，該指令第 4 章，即第 25 條、第 26 條規定，已建立制度確保會員國對個人資料傳輸至第三國予以監督。此一制度係對該指令第 2 章建立之一般制度，即個人資料處理規則合法性的補充 (請參考判決 *Lindqvist*, C-101/01, EU:C:2003:596, 第 63 段)。

47 As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

依據憲章第 8 條第 3 項及第 95/46 號指令第 28 條，國家監管機關負責監督個資處理之保護是否符合歐盟規定，是以，國家監管機關有權檢查該會員國向第三國傳輸個人資料是否符合第 95/46 號指令。

48 Whilst acknowledging, in recital 56 in its preamble, that transfers of personal data from the Member States to third countries are necessary for the expansion of international trade, Directive 95/46 lays down as a principle, in Article 25(1), that such transfers may take place only if the third country ensures an adequate level of protection.

在第 95/46 號指令前言第 56 點，雖然承認從會員國傳輸個人資料至第三國，對於國際貿易的拓展是有其必要，但第 95/46 號指令在第 25 條第 1 項立下一個原則，只有在第三國確保適足程度的保護下，始得為該傳輸。

49 Furthermore, recital 57 states that transfers of personal data to third countries not ensuring an adequate level of protection must be

prohibited.

更甚者，該指令前言第 57 點指出傳輸個人資料至第三國，如無法確保適足程度的保護，應該被禁止。

50 In order to control transfers of personal data to third countries according to the level of protection accorded to it in each of those countries, Article 25 of Directive 95/46 imposes a series of obligations on the Member States and the Commission. It is apparent, in particular, from that article that the finding that a third country does or does not ensure an adequate level of protection may, as the Advocate General has observed in point 86 of his Opinion, be made either by the Member States or by the Commission.

為了根據各國保護程度控管個人資料傳輸至第三國的行為，第 95/46 號指令第 25 條課予會員國及執委會一系列之義務。特別是從該條規定來看，如同佐審官意見第 86 點所述，由會員國或執委會決定第三國是否確保適足程度之保護。

51 The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in *Albako Margarinefabrik*, 249/85, EU:C:1987:245, paragraph 17, and *Mediaset*, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

執委會依歐盟第 95/46 號指令第 25 條第 6 項規定，得通過認定第三國確保適足保護程度之決定，並依該指令第 25 條第 6 項第 2 款規定，該決定應對會員國提出，會員國須採取必要措施以遵守該決定。依歐盟運作條約第 288 條第 4 項規定，該「產生許可將個人資料自會員國傳輸至該第三國之效力」的決定將拘束所有

會員國，並因此拘束會員國內全體機關（構） (相關影響得參考判決 Albako Margarinefabrik, 249/85, EU:C:1987:245 第 17 段，以及 *Mediaset*, C-69/13, EU:C:2014:71 第 23 段)。

52 Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in *Commission* v *Greece*, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

因此，在執委會的決定被法院宣告無效之前，所有會員國及其機關（構），包含其獨立監管機關，顯然無法採取與該決定相反之措施，例如不受該決定拘束而否定第三國確保適足的保護程度。歐盟機構所採取之措施除非遭撤銷、廢除，或於先行裁決或違法答辯程序中經宣告無效，否則原則上該措施將推定為合法，並因此產生法律效果(判決如 *Commission* v *Greece*, C-475/01, EU:C:2004:585, 第 18 段 及其引用之案例法)。

53 However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

然而，執委會依歐盟第 95/46 號指令第 25 條第 6 項規定通過之決定，例如歐盟第 2000/520 號決定，不能妨礙其個資已經或可能被傳輸至第三國之人，依該指令第 28 條第 4 項向國內監管機關提出就其個資處理有關之權利及自由的申訴。正如佐審官特別在其意見第 61 點、第 93 點和第 116 點指出，歐盟的決定不能排除或減損歐盟基本權利憲章第 8 條第 3 項及該指令第 28 條賦予國家監管機關的權力。

54 Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.

無論是歐盟基本權利憲章第 8 條第 3 項或歐盟第 95/46 號指令第 28 條，均不排除國家監管機關監督個資傳輸至屬於歐盟第 95/46 號指令第 25 條第 6 項決定之第三國的權限。

55 In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.

特別依歐盟第 95/46 號指令第 28 條第 4 項第 1 款規定，國家監管機關應受理「由當事人提出就其個資處理有關之權利及自由保護的申訴」，即便是對於執委會依該指令第 25 條第 6 條通過之決定亦不例外。

56 Furthermore, it would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of preventing a national supervisory authority from examining a person's claim concerning the protection of his rights and freedoms in regard to the processing of his personal data which has

been or could be transferred from a Member State to the third country covered by that decision.

再者，若謂執委會依歐盟第 95/46 號指令第 25 條第 6 項規定通過之決定，具有「排除國家監管機關在當事人之個資已經或將要自會員國傳輸至該決定涵蓋之第三國時，審查與當事人個資處理有關之權利及自由保護的申訴」之效力，此將與歐盟第 95/46 號指令建立的制度及第 25 條和第 28 條之目的相牴觸。

57 On the contrary, Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data. Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

相反的，歐盟第 95/46 號指令第 28 條依其性質適用於任何個資處理行為。因此，即使是執委會依該指令第 25 條第 6 項通過之決定，當國家監管機關受理由當事人提出就其個資處理有關之權利及自由保護的申訴時，必須能完全獨立地審查該個資傳輸行為是否符合指令的要求。

58 If that were not so, persons whose personal data has been or could be transferred to the third country concerned would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 68).

倘非如此，對於個資已經或可能被傳輸至第三國之人而言，無疑剝奪其依歐盟基本權利憲章第 8 條第 1 項及第 3 項所保障得向國家監管機關提出申訴以保護其基本權利（參見 *Digital Rights Ireland and Others*，C293 / 12 和 C594 / 12，EU：C：2014：238，第 68 段）。

59 A claim, within the meaning of Article 28(4) of Directive 95/46, by which a person whose personal data has been or could be transferred to a third country contends, as in the main proceedings, that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 25(6) of that directive, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

對於由其個資已經或可能被傳輸至第三國之人，依歐盟第 95/46 號指令第 28 條第 4 項規定提出之申訴，如同本案訴訟程序般，儘管執委會已在依該指令第 25 條第 6 款通過之決定中作出認定，惟若該國的法律與實踐無法確保適足的保護程度時，此應理解為對於該決定本質上是否足以保護個人隱私、基本權與自由構成疑慮。

60 In this connection, the Court's settled case-law should be recalled according to which the European Union is a union based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights (see, to this effect, judgments in *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 66; *Inuit Tapiriit Kanatami and Others* v *Parliament and Council*, C-583/11 P, EU:C:2013:625, paragraph 91; and *Telefónica* v *Commission*, C-274/12 P, EU:C:2013:852, paragraph 56). Commission decisions adopted pursuant to Article 25(6) of Directive 95/46 cannot therefore escape such review.

基於歐盟是個法治的聯盟，所屬機構的所有行為皆應接受審查是否與條約、一般法律原則及基本權利相符。（相關影響得參考判決 *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518 第 66 段； *Inuit Tapiriit Kanatami and Others* v *Parliament and Council*, C-583/11 P, EU:C:2013:625 第 91 段；以及 *elefónica* v *Commission*, C-274/12 P, EU:C:2013:852 第

56 段）。執委會依歐盟第 95/46 號指令第 25 條第 6 項通過之決定亦不得免於審查。據此，本案應回顧相關的法院案例。

61 That said, the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in *Melki and Abdeli*, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and *CIVAD*, C-533/10, EU:C:2012:347, paragraph 40).

也就是說，僅本院有權宣告歐盟的行為，例如依歐盟第 95/46 號指令第 25 條第 6 項通過之決定，是否為無效。此排他性的管轄權限是為藉由確保歐盟法律統一適用以保障法律之明確性（參見 *Melki and Abdeli*, C-188/10 及 C-189/10, EU:C:2010:363 第 54 段，以及 *CIVAD*, C-533/10, EU:C:2012:347, 第 40 段）

62 Whilst the national courts are admittedly entitled to consider the validity of an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, they are not, however, endowed with the power to declare such an act invalid themselves (see, to this effect, judgments in *Foto-Frost*, 314/85, EU:C:1987:452, paragraphs 15 to 20, and *IATA and ELFAA*, C-344/04, EU:C:2006:10, paragraph 27). A fortiori, when the national supervisory authorities examine a claim, within the meaning of Article 28(4) of that directive, concerning the compatibility of a Commission decision adopted pursuant to Article 25(6) of the directive with the protection of the privacy and of the fundamental rights and freedoms of individuals, they are not entitled to declare that decision invalid themselves.

儘管國內法院有權檢視歐盟行為的有效性，例如依歐盟第 95/46 號指令第 25 條第 6 項通過之決定，但無權宣告此類行為無效（參見 *Foto-Frost*，314/85，EU：C：1987：452，第 15 至 20 段，*IATA and ELFAA*，C 344/04，EU：C：2006：10 第 27 段）。至於國家監管機關依指令第 28 第 4 項審查執委會依該指令第 25 條第 6

項通過之決定是否足以確保個人隱私、基本權與自由之保護的申訴時，更無權宣告該決定無效。

63 Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

綜上所述，當一個人的個資已經或可能被傳輸至執委會依歐盟第 95/46 號指令第 25 條第 6 項通過之決定涵蓋的第三國，其並向國家監管機關就個資處理有關之權利及自由保護提出申訴，且在申訴中，如同本案訴訟程序，質疑該決定是否足以確保個人隱私、基本權與自由之保護時，國家監管機關有義務盡最大努力審查其申訴。

64 In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in *T & L Sugars and*

Sidul Açúcares v *Commission*, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

當國家監管機關認為該申訴所憑論據並無理由而駁回時，依歐盟基本權利憲章第 47 條解釋之歐盟第 95/46 號指令第 28 條第 3 項第 2 款規定，提出申訴之人應得向國內法院尋求司法救濟以就對其產生不利影響之決定提出異議。參酌本判決第 61 段和第 62 段引用之判例法，國內法院如就決定之無效性認為當事人之主張或如同本案，自行於動議中提出的一個或數個根據係有理由時，應停止訴訟程序並請求本院就該決定之有效性作出先決判決。（參見判決 *T & L Sugars and Sidul Açúcares* v *Commission*，C 456/13 P，EU：C：2015： 284，第 48 段及其引用之判例法）。

65 In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. 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.

相反的，如國家監管機關認為申訴者對個資處理有關之權利及自由保護的申訴係有理由時，依歐盟基本權利憲章第 8 條第 3 項解釋之歐盟第 95/46 號指令第 28 條第 3 項第 1 款第 3 目規定，國家監管機關應得參與法律訴訟程序。國家立法機構有義務提供法律救濟途徑，使國家監管機關如同樣認為執委會決定之有效性存有疑慮時，得將該異議向國內法院提出，以對審查該決定之有效性的先決判決提出參考意見。

66 Having regard to the foregoing considerations, the answer to the questions referred is that Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

基於上開考量，該爭點之答案應為，依歐盟基本權利憲章第 7 條、第 8 條和第 47 條解釋之歐盟第 95/46 號指令第 25 條第 6 項規定，須理解為依該條款通過之決定，例如歐盟第 2000/520 號決定，即執委會認定第三國已確保適足的保護程度，並未排除會員國的監管機關依該指令第 28 條規定，審查「其個資自會員國傳輸至該第三國之當事人，聲稱該第三國的現行法律與實踐無法確保適足的保護程度，因而就個資處理有關之權利與自由保護提出的申訴」之權力。

The validity of Decision 2000/520

2000/520 決定之有效性

67 As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in

order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

從提交法院對提交問題的解釋可以明顯看出，Schrems 先生在訴訟程序主張，美國的法律和實踐不能確保符合歐盟第 95/46 號指令第 25 條之適足保護程度。正如佐審官在他的意見第 123 點和第 124 點指出，Schrems 先生以及提交法院均對歐盟第 2000/520 號決定之有效性表示懷疑。於此情形，考慮到本判決第 60 至 63 段所載的內容，並為給予提交法院完整回覆，應審查該決定是否符合歐盟基本權利憲章解釋之歐盟第 95/46 號指令。

The requirements stemming from Article 25(6) of Directive 95/46

歐盟第 95/46 號指令第 25 條第 6 項之規定

68 As has already been pointed out in paragraphs 48 and 49 of the present judgment, Article 25(1) of Directive 95/46 prohibits transfers of personal data to a third country not ensuring an adequate level of protection.

正如本判決第 48 段和第 49 段所指出，歐盟第 95/46 號指令第 25 條第 1 項禁止個資傳輸至無法確保適足保護程度之第三國。

69 However, for the purpose of overseeing such transfers, the first subparagraph of Article 25(6) of Directive 95/46 provides that the Commission 'may find … that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into …, for the protection of the private lives and basic freedoms and rights of individuals'.

然而，為了監管此類傳輸，歐盟第 95/46 號指令第 25 條第 6 項第 1 款規定，執委會得基於第三國之國內法或國際承諾，認定第三國足以確保本條第 2 項對於保護私人生活及基本自由與權利之適足保護程度。

70 It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an

adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

誠然，歐盟第 95/46 號指令第 25 條第 2 項或其他條款均未對適足保護程度概念提供定義。特別是第 25 條第 2 項僅說明「應依照所有單一或一系列傳輸個資行為的情況以評估」第三國提供的保護程度適足性，並例示在評估時必須考量之情況。

71 However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'.

然而，首先，從歐盟第 95/46 號指令第 25 條第 6 項文義可知，該條款要求第三國依其國內法或其國際承諾「確保」適足的保護程度。其次，依同一條款，第三國確保的保護適足性是基於「保護個人私人生活和基本自由與權利」而予評估。

72 Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

因此，歐盟第 95/46 號指令第 25 條第 6 項係為實踐歐盟基本權利憲章第 8 條第 1 項規定保護個人資料的明確義務，以及如佐審官於其意見第 139 點所述，意在確保於個資傳輸至第三國的情形仍維持此高程度的保護。

73 The word ‘adequate’ in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, 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. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

歐盟第 95/46 號指令第 25 條第 6 項所謂「適足」一詞，的確表示並非要求第三國確保其保護程度與歐盟法律秩序完全相同。然而，正如佐審官於其意見第 141 點指出，「適足的保護程度」應理解為要求第三國依其國內法或其國際承諾，於事實上確保其保護程度與依歐盟基本權利憲章解釋之歐盟第 95/46 號指令實質相同。若無此要求，本判決前揭目的將遭忽視，且依歐盟基本權利憲章解釋之歐盟第 95/46 號指令所保障的高程度保護，將輕易的被以「為在第三國處理個資而將個人資料自歐盟傳輸至該第三國」的方式規避。

74 It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with,

those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

由歐盟第 95/46 號指令第 25 條第 6 項用詞可以明顯看出，執委會決定所涵蓋之第三國的法律秩序須能確保適足的保護程度。即便第三國在此為達到該保護程度的方法，可能與歐盟為確保遵循依歐盟基本權利憲章解釋之歐盟第 95/46 號指令所採取之方式有所不同，該方法仍須經證明於實踐上具有效性，以確保其保護程度與歐盟之保障實質相同。

75 Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

因此，既然執委會依歐盟第 95/46 號指令第 25 條第 2 項規定，須考量傳輸個資至第三國的所有情況，在審查第三國提出的保護程度時，即有義務評估該第三國依國內法或國際承諾所適用的法規，以及確保遵循該法規的實踐方式。

76 Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

又鑒於第三國確保的保護程度可能發生變化，執委會依歐盟第 95/46 號指令第 25 條第 6 項通過決定後，有義務定期檢視第三國之保護程度於事實上和法律上仍為正當。在任何情況下，當有證據足構成對前述情形之懷疑時，此檢視即為必要。

77 Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

此外，正如佐審官於其意見第 134 點和第 135 點所述，審查依歐盟第 95/46 號指令第 25 條第 6 項通過之執委會決定的有效性時，亦須考量於該決定通過後始發生之情形。

78 In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).

據此，由於保護個資的重要功能是為尊重私人生活的基本權利，且如將個資傳輸至未能確保具有適足的保護程度之第三國時，將有大量人民之基本權利為此受到侵害，因此，執委會應依照按歐盟基本權利憲章解釋之歐盟第 95/46 號指令第 25 條規定，嚴格認定第三國保護程度之適足性是否有所減損（參見判決 *Digital Rights Ireland and Others*，C293 / 12 和 C594 / 12，EU：C：2014 ：238，第 47 段和第 48 段）。

Article 1 of Decision 2000/520

歐盟第 2000/520 號決定第 1 條

79 The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance

with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

執委會於歐盟 2000/520 號決定第 1 條第 1 項認為，附件 1 所列之原則如依附件 2 所列常見問答以執行，即可確保對從歐盟傳輸至設立於美國之組織的個人資料提供適足程度的保護。從該條款中可知，此原則和常見問答均由美國商務部發布。

80 An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

依歐盟第 2000/520 號決定第 1 條第 2 項及第 3 項，並參照附件 2 所列的常見問答 6 可知，組織應自我證明符合安全港原則。

81 Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

第三國採取自我證明制度並不違反歐盟第 95/46 號指令第 25 條第 6 項之要求，即第三國「以其國內法或國際承諾」確保適當之保護程度，此制度之可靠性立基於有效檢測和監督機制，使任何違反基本權利保護—特別是尊重私人生活和個資保護權利—之行為均能被識別並予以處罰。

82 In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are 'intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'. Those principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

以此處為例，依歐盟第 2000/520 號決定附件 1 第 2 段的規定，安全港原則「僅供接受歐盟傳輸之個資的美國組織導入該原則並受適足性之推定」。因此，此原則僅適用於自我證明之美國組織，美國公務機關則無須遵守。

83 Moreover, Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

此外，依其第 2 條說明，歐盟第 2000/520 號決定「僅關於依常見問答實施[安全港原則]即可認定美國符合歐盟第 95/46 號指令第 25 條第 1 項規定之保護適足性」，卻未有足夠證據顯示美國依其國內法或其國際承諾已具備符合該指令第 25 條第 6 項所指之適足保護程度的措施。

84 In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising

any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'.

又根據歐盟第 2000/520 號決定附件 1 第 4 段，安全港原則之適用性可能受有限制，特別是為了滿足國家安全、公共利益或執法要求之必要程度，和依法律、政府法規或案例法而產生衝突義務，或經明確授權，且於行使此類授權時，組織可證明係於必要範圍的限制內，為凌駕安全港原則的正當利益而違反安全港原則。

85 In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

對此，歐盟第 2000/520 號決定附件 4 的 B 部分指出「在依美國法律而面臨衝突義務時，無論是否導入安全港原則的美國組織均應遵守法律」。

86 Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

因此，歐盟第 2000/520 號決定稱「國家安全、公共利益或執法要求」優先於安全港原則，故自歐盟接收個資之自我證明的美國組織，當面臨衝突義務時必須忽視該原則，將牴觸該原則之要求。

87 In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with

the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).

鑒於歐盟第 2000/520 號決定附件 1 第 4 段規定的例外規定，該決定對於個資已經或可能自歐盟傳輸至美國的當事人之基本權利，得以國家安全和公共利益要求或美國國內立法加以干涉，此對私人生活基本權利之干涉不分所涉及之私人生活資訊是否敏感，或者相關人等是否因而面臨不利後果（判決 *Digital Rights Ireland and Others*，C 293/12 和 C 594/12，歐盟：C：2014：238，第 33 段和引用之判例法）。

88 In addition, Decision 2000/520 does 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 authorised to engage in when they pursue legitimate objectives, such as national security.

此外，歐盟第 2000/520 號決定未包含美國為追求合法目的，例如國家安全，而干涉從歐盟傳輸個資之當事人的基本權利之任何相關限制性法規。

89 Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings

with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

歐盟第 2000/520 號決定也未提及防止此種干涉之保護法律。正如佐審官於其意見第 204 點至第 206 點指出，聯邦貿易委員會的處理程序（特別是該決定附件 2 中常見問答 11 中所述的程序，僅限於商業糾紛）與私人紛爭解決機制，僅與美國企業遵守安全港原則有關，尚無法適用於涉及國家措施干預基本權利之紛爭。

90 Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

此外，上述對歐盟第 2000/520 號決定之分析是執委會自行證明對於執行該決定所生之結果。特別是政策文件 COM（2013）846 號第 2 點和第 3.2 點，以及政策文件 COM（2013）847 號中的第 7.1 點、第 7.2 點和第 8 點，其內容見本判決第 13 段至第 16 段以及第 22 段、第 23 段和第 25 段，執委會發現，美國當局能取得從會員國傳輸之個資，並以保護程度不相符之方式處理該資料，且與傳輸目的相比，已超出與國家安全保護所應有之嚴格必要性及比例原則。此外執委會指出，個資當事人並無行政或司法救濟手段，特別是與其有關的資料遭取得時，得以糾正或刪除。

91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

關於歐盟境內對基本權利和自由的保護程度，凡涉及干預歐盟基本權利憲章第 7 條和第 8 條保障之基本權利，歐盟於訂定法律時必須以法院確定之判例，制定明確和準確的規則，以規範干預之範圍及必須採取之最低限度。如此個資當事人即可獲得足夠保護，以有效降低其個資遭濫用或非法取得之風險。當個資面臨自動化方式處理，或遭非法獲取之重大風險時，此類的保護措施需求將大增（判決詳 *Digital Rights Ireland and Others*，C293 / 12 和 C594 / 12，歐盟 ：C：2014：238，第 54 段和第 55 段以及引用之判例法）。

92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

尤其是，歐盟基於對私人生活的尊重而要求的基本權保護，在個資保護方面，僅限於絕對必要之情況，始能適用排除及限制之規定（判決詳 *Digital Rights Ireland and Others* C 293/12 和 C 594/12，歐盟：C：2014：238，第 52 段和引用之判例法）。

93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

立法並未限制於嚴格必要的情況下始得儲存自歐盟傳輸至美國的所有人的所有個人資料，即廣泛許可而未依據追求之目的設有任何區別、限制或例外，亦未依照具體、嚴格限制且可正當化干預行為之目的而制定判斷公務機關存取該資料及後續利用的客觀標準。（相關影響，參見歐洲議會和歐盟理事會 2006 年 3 月 15 日關於保留公共電信服務或公共通信網路產生之資料歐盟指令第 2006/24 / EC 號，以及修正歐盟指令第 2002/58 / EC 號（OJ 2006 L 105，第 54 頁），判決 *Digital Rights Ireland and Others*，C 293/12 和 C 594/12，EU：C：2014：238，第 57 段至第 61 段）。

94 In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

特別是允許公務機關廣泛取得電子通信內容之立法，應視為侵害歐盟基本權利憲章第 7 條所保障尊重私人生活之基本權利的本質（相關影響得參照，*Digital Rights Ireland and Others*，C 293/12 和 C 594/12，EU：C：2014：238，第 39 段）。

95 Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in *Les Verts* v *Parliament*, 294/83, EU:C:1986:166, paragraph 23; *Johnston*, 222/84, EU:C:1986:206, paragraphs 18 and 19; *Heylens and Others*, 222/86, EU:C:1987:442, paragraph 14; and *UGT-Rioja and Others*, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

同樣地，立法亦未提供任何可能，使個人得以尋求法律救濟以取得、更正、刪除其個人資料，亦有違歐盟基本權利憲章第 47 條之要求，即未尊重「獲得有效司法保護」此基本權之本質。歐盟基本權利憲章第 47 條第 1 項規定，任何因他人違反歐盟法律保障之權利和自由而受害之人，均有權依該條規定於法庭獲得有效救濟。為確保歐盟法律被遵守而設計的有效司法審查制度，即包含於該法律規範之中（相關影響參見判決 *Les Verts* v *Parliament*，294/83，EU：C：1986： 166，第 23 段; *Johnston*，222/84，EU：C：1986：206，第 18 和 19 段; *Heylens and Others*，222/86，EU：C：1987：442 第 14 段;以及 *UGT-Rioja and Others* 等，C 428/06 至 C 434/06，EU：C：2008：488，第 80 段）。

96 As has been found in particular in paragraphs 71, 73 and 74 of the present judgment, in order for the Commission to adopt a decision

pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment.

如本判決第 71 段、第 73 段及第 74 段特別指出，執委會依歐盟第 95/46 號指令第 25 條第 6 項通過之決定，必須具備充分理由以明確說明第三國國內法或國際承諾已確保對於基本權利的保護程度與歐盟法秩序所保障者實質相同，此保護程度已於本判決前揭段落中說明。

97 However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

然而，執委會在歐盟第 2000/520 號決定並未說明美國依其國內法或國際承諾已確保符合適足的保護程度。

98 Consequently, without there being any need to examine the content of the safe harbour principles, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid.

因此，無需審查安全港原則的內容，便可以得出歐盟第 2000/520 號決定第 1 條因不符依歐盟基本權利憲章解釋之歐盟第 95/46 號指令第 25 條第 6 項規定的結論，因而無效。

Article 3 of Decision 2000/520

歐盟第 2000/520 號決定第 3 條

99 It is apparent from the considerations set out in paragraphs 53, 57 and 63 of the present judgment that, under Article 28 of Directive 95/46, read in the light in particular of Article 8 of the Charter, the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a

person's rights and freedoms in regard to the processing of personal data relating to him. That is in particular the case where, in bringing such a claim, that person raises questions regarding the compatibility of a Commission decision adopted pursuant to Article 25(6) of that directive with the protection of the privacy and of the fundamental rights and freedoms of individuals.

由本判決前揭第 53 段、第 57 段及第 63 段所述之考量可知，依歐盟基本權利憲章第 8 條解釋之歐盟第 95/46 號指令第 28 條規定，國家監管機關必須能夠完全獨立的審查當事人對處理其個人資料有關的權利與自由之保護的任何申訴。尤其是當事人於該申訴中質疑執委會依該指令第 25 條第 6 項通過之決定是否足以保護個人之隱私及基本權與自由的情況。

100 However, the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

然而，歐盟第 2000/520 號決定第 3 條第 1 項第 1 款依照執委會按歐盟第 95/46 號指令第 25 條之意認定的適足保護程度，對國家監管機關的權力訂有特殊規定。

101 Under that provision, the national supervisory authorities may, '[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]', under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

據該條款，國家監管機關得「…中止資料傳輸至自我證明遵守[歐盟第 2000/520 號決定之原則]的組織，且不妨礙其為確保該國依

據歐盟指令[95/46]（第 25 條除外）所定之國家法規的遵循性而採取特定措施之權力」，係以限制條件建立監管機關介入的高門檻。雖然該條款不妨礙監管機關為確保該國依據歐盟指令[95/46]所定之國家法規的遵循性而採取特定措施之權力，但另一方面卻排除監管機關為確保該指令第 25 條的遵循性而採取特定措施的可能。

102 The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

因此，在當事人依歐盟第 95/46 號指令第 28 條規定提出申訴，而申訴內容係質疑執委會依該指令第 25 條第 6 項作出認定第三國已確保適足保護程度之決定，是否足以保護個人之隱私及基本權與自由的情形時，歐盟第 2000/520 號決定第 3 條第 1 項第 1 款應理解為排除歐盟第 95/46 號指令第 28 條賦予國家監管機關之權力。

103 The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

歐盟立法機關授予執委會於歐盟第 95/46 號指令第 25 條第 6 項之執行權，並不包含有權限制本判決前述國家監管機關之權力。

104 That being so, it must be held that, in adopting Article 3 of Decision 2000/520, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46, read in the light of the Charter, and that Article 3 of the decision is therefore invalid.

因此可認定，執委會於通過歐盟第 2000/520 號決定第 3 條時，已逾越依歐盟基本權利憲章解釋之歐盟第 95/46 號指令第 25 條第 6 項所賦予的權力，因此該決定第 3 條無效。

105 As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety.

由於歐盟第 2000/520 號決定第 1 條和第 3 條與第 2 條和第 4 條及其附件不可分割，其無效性及於整體決定。

106 Having regard to all the foregoing considerations, it is to be concluded that Decision 2000/520 is invalid.

綜上所述，歐盟第 2000/520 號決定無效。

Costs

裁判費用

107 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

由於對本案當事人而言，本（先決裁決）程序係提交法院暫停訴訟之步驟，應由該法院決定當事人應負擔之費用。另，除當事人外，於程序中向本院提交意見所產生之費用將不予退還。

On those grounds, the court(Grand chamber) hereby rules:

基於上述理由，本法院（大分庭）判決如下：

1. Article 25(6) of 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 as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that

provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

歐洲議會與歐盟理事會於 1995 年 10 月 24 日個資處理與自由傳輸之個資保護會議通過，後經歐洲議會與歐盟理事會於 2003 年 9 月 29 日會議修正（No 1882/2003），並依歐盟基本權利憲章第 7 條、第 8 條和第 47 條解釋之歐盟第 95/46/EC 號指令第 25 條第 6 項，須理解為依該條款通過之決定，例如執委會在 2000 年 7 月 26 日依據第 95/46 號指令，就安全港隱私原則及美國商務部發布之相關常見問答構成的保護適足性作成之歐盟第 2000/520 號決定，即執委會認定第三國已確保適足的保護程度，並未排除會員國的監管機關依該指令第 28 條修正後之規定，審查「其個資自會員國傳輸至該第三國之當事人，聲稱該第三國的現行法律與實踐無法確保適足的保護程度，因而就個資處理有關之權利與自由保護提出的申訴」之權力。

2. Decision 2000/520 is invalid.

歐盟第 2000/520 號決定無效。