金融與徵信叢書 NO.77

歐盟個人資料保護規則

財團法人金融聯合徵信中心
Joint Credit Information Center

歐盟個人資料保護規則
【金融與徵信叢書 NO.77】

序

歐洲聯盟於 1995 年 10 月 24 日制訂第 95/46/EC 號指令，即一般通稱之歐盟「個人資料保護綱領」（Data Protection Directive），於施行逾二十年後，為確保對當事人一致而高度之保護，建構更為周密之資料保護框架，歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過第 2016/679 號「個人資料保護規則」（General Data Protection Regulation）及附屬規定，自 2018 年 5 月 25 日起於歐盟各會員國直接施行，取代前揭由會員國制訂國內法施行之「個人資料保護綱領」。

近年來隨著科技的快速發展及全球化，資料控管或處理者蒐集、處理與利用個人資料之規模顯著提升，帶來許多新的議題與挑戰，「個人資料保護規則」可謂歐盟對前述議題的處理與回應，諸如：重新建構並明定資料主體的「被遺忘權」（right to be forgotten）與「拒絕權」（right to object），以及資料控管或處理者的制度性義務，包括資料保護員（data protection officer）的指定、「設計與預設」資料保護原則的遵守、資料保護影響評估的執行等，對我國處理相關議題深具參考價值。

爰此，聯徵中心特委託萬國法律事務所譯介歐盟「個人資料保護規則」，以借鑑歐盟個人資料保護之制度經驗，並凝聚我國對於個人資料保護相關法制變革與制度運作之社會共識。今後聯徵中心仍當本諸服務社會之職志，編訂金融與徵信叢書廣為推行，尚祈對我國整體金融市場與法制環境之健全發展有所裨益，並請各界先進不吝斧正。

財團法人金融聯合徵信中心　敬具

2017 年 7 月

目　錄

歐盟「個人資料保護規則」導讀

蔡柏毅 *

壹、歐盟個人資料保護法制發展

歐洲聯盟基本權利憲章（Charter of Fundamental Rights of the European Union）第 8 條第 1 項及歐洲聯盟運作條約（Treaty on the Functioning of the European Union）第 16 條均規定，任何人均有保護其個人資料之權利。爰此，歐洲議會及歐盟理事會於 1995 年 10 月 24 日制訂歐盟指令第 95/46/EC 號，於施行逾廿載後，再度領先世界潮流，於 2016 年 4 月 27 日通過歐盟規則第 2016/679 號「個人資料保護規則（General Data Protection Regulation）[1]」，取代前揭 95/46/EC 號歐盟指令，並自 2018 年 5 月 25 日起施行。

歐盟指令第 95/46/EC 號所揭示之宗旨及保護原則雖仍屬健全，惟僅係最低限度之保護規範，歐盟各會員國於歐盟指令第 95/46/EC 號基礎上所建立之個人資料保護制度，對當事人權利保護程度之差異，可能因此阻礙歐盟對於經濟活動之執行、造成不當競爭及妨礙機關根據歐盟法所應履行之職責。為確保對當事人一致且高度之保護，並排除個人資料在歐盟間流通之阻礙，本規則關於資料處理之個人權利及自由之保護程度於全體會員國間係一體適用，以建構強力且更一致之資料保護框架。

---

* 本文係財團法人金融聯合徵信中心「歐盟個人資料保護規則暨相關規定委外翻譯專案」，法規版本為歐盟網頁揭載之英文版條文，中譯部分委由萬國法律事務所提供，惟相關採擇如有誤謬，文責仍當由作者自負。（作者為金融聯合徵信中心法務室專員）

1 歐盟「個人資料保護規則」之名稱為暫譯。如未特別標示，本文簡稱為「本規則」者，及直接引述各條（項、款）號者，均係指涉此一歐盟規則而言。

貳、歐盟「個人資料保護規則」章節一覽

第一章　總則（General provisions）

第二章　原則（Principles）

第三章　資料主體之權利（Rights of the data subject）

　　第一節　透明度及管道（Transparency and modalities）

　　第二節　個人資料之資訊與接近使用（Information and access to personal data）

　　第三節　更正及刪除（Rectification and erasure）

　　第四節　拒絕權及個人化之自動決策（Right to object and automated individual decision-making）

　　第五節　限制（Restrictions）

第四章　控管者及處理者（Controller and processor）[2]

　　第一節　一般義務（General obligations）

　　第二節　個人資料之安全（Security of personal data）

　　第三節　資料保護影響評估（Data protection impact assessment）

　　第四節　資料保護官員（Data protection officer）

　　第五節　行為守則與認證（Codes of conduct and certification）

第五章　個人資料傳輸至第三國或國際組織（Transfers of personal data to third countries or international organisations）

第六章　獨立監管機關（Independent supervisory authorities）

　　第一節　獨立地位（Independent status）

---

[2] 依本規則第 4 條之定義，「控管者」（controller）係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；「處理者」（processor）指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構。區別在於處理者不直接決定蒐集、處理個人資料的特定目的與方法，而是依控管者的指示操作。95/46/EC 號歐盟指令未直接規範處理者，僅要求控管者必須透過契約要求處理者遵守相關規定，本規則直接要求控管者及（某些情形下的）處理者都必須確實符合相關規定。

參、歐盟「個人資料保護規則」之規範重點

一、個人資料處理之一般性原則（第 5 條）

個人資料保護之一般原則為尊重權利主體之基本權及自由，尤其是保護個人資料之權利，不問其國籍或住居所而有差異。然而，個人資料之保護並非絕對，必須考慮社會的機能與作用，依照比例原則，平衡兼顧其他基本權利，特別是尊重個人及家庭、住居、通訊、思想、良心及宗教自由、言論及資訊自由、職業自由、受有效之救濟及公正審判之權利，及文化、宗教及語言之多元性保障等。依本規則第 5 條之規定，個人資料處理應遵循之原則如下：

- 合法性、公正性及透明度（lawfulness, fairness and transparency）原則，即對資料主體為合法、公正及透明之處理；
- 目的限制（purpose limitation）原則，即蒐集目的須特定、明確及合法正當（specified, explicit and legitimate purposes），且不得為目的以外之進階處理；

[3] 本章規範各種特殊類型個人資料處理，包括：處理與言論及資訊自由、官方文件之處理與公眾接近使用、國民識別證字號之處理、僱傭關係下之處理及為實現公共利益、基於科學或歷史研究目的或統計目的所為處理之保護措施及例外規定等等。

- 資料最少蒐集（data minimisation）原則，即處理個人資料應適當、相關且限於處理目的所必要（adequate, relevant and limited to what is necessary in relation to the purposes）者；
- 正確性（accuracy）原則，即應採取一切措施，以確保不正確之個人資料立即被刪除或更正；
- 儲存限制（storage limitation）原則，即保存個人資料不得長於處理目的所必要之期間；
- 完整及保密（integrity and confidentiality）原則：即處理個人資料之方式應具適當安全性，包括技術上及組織上措施，以有效防止未經授權或非法之處理、遺失、破壞或損壞；
- 課責（accountability）原則，即個人資料控管者應確實遵守上述原則，並就其符合相關原則負舉證責任。

二、例外不適用本規則之情形（第 2 條）

本規則要求歐盟各會員國應調和其內國法包括新聞、學術、藝術及或文學表達等表意自由、資訊自由與個人資料保護之權利。在必須調和個人資料受保護之權利與表意與資訊自由時，專為新聞、學術、藝術或文學表達目的所為之個人資料處理，應得除外或豁免於本規則之規定，尤適用於視聽領域、新聞檔案及媒體資料庫之資料處理。依本規則規定，下列個人資料之處理不適用本規則：

- 歐盟法以外治權領域之活動（outside the scope of Union law）；
- 當事人所為單純之個人或家庭活動（purely personal or household activity）；
- 主管機關為預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的（包括為維護及預防對於公共安全造成之威脅）所為之個人資料處理。

三、個人資料處理之合法要件（第 6 條）

合法之個人資料處理應至少符合下列要件之一：

- 資料主體同意為一個或多個特定目的處理其個人資料；
- 處理係為向身為契約當事人之資料主體履行契約所必須者，或在締

約前，應資料主體之要求，所必須採取之步驟；

- 處理係控管者為遵守法律義務所必須者；
- 處理係為保護資料主體或他人之重大利益所必須者；
- 處理係為符合公共利益執行職務或行使公權力所必須者；
- 處理係控管者或第三者為追求正當利益（legitimate interests）之目的所必須者，但該資料主體之利益、基本權或自由優先於該等利益，特別是該資料主體為兒童時，不適用之。

上述個人資料處理之特定目的應具明確性（explicit）及合法性（legitimate），並於蒐集個人資料時確定並告知當事人。個人資料應適當、相關及限於處理目的之必要範圍內（adequate, relevant and limited to what is necessary for the purposes），並確保個人資料之儲存期間在最小限度範圍。個人資料之處理係以直接行銷為目的時，資料主體應有權在任何時間、且毋需任何費用拒絕該處理，包括在與直接行銷有關之範圍內建檔，且不問係原始處理或進階處理。

為符合公共利益、達成科學或歷史研究目的或統計目的所為個人資料之處理，應受本規則所定適當保護措施之拘束。該等保護措施應確保備妥技術上及組織上之措施，特別是資料最少蒐集原則之落實。前述統計目的意指資料處理結果不是個人資料，而係總體資料（aggregate data），且該結果或個人資料並非用於支持關於任何特定當事人之措施或決定。

四、同意之合法要件（第 7 條）

同意之給予必須是資料主體依其意思決定就其個人資料處理所為具體、肯定、自由、明確、受充分告知及非模糊之指示，如：口頭或書面之聲明，包括以電子方式為之者[4]。如單純沉默、預設選項為同意

[4] 依本規則第 4 條之定義，「同意」（consent）係指資料主體基於其意思，透過聲明（statement）或明確肯定之行動（clear affirmative action），所為具自主性（freely given）、具體（specific）、知情（informed）及明確（unambiguous）之表示同意處理與其有關之個人資料。的指示操作。95/46/EC 號歐盟指令未直接規範處理者，僅

（pre-ticked boxes）或不為表示等，均不構成同意。同意須涵蓋基於相同之一個或多個目的所為之全部處理活動，如資料之處理具有多重目的時，全部目的均應取得同意。

個人資料處理係基於資料主體之同意者，控管者應舉證證明資料主體之同意，確保資料主體知悉同意之事實及範圍。事先擬定之同意聲明書，應以易懂（intelligible）且便於取得（easily accessible）之格式為之，並使用清晰易懂（clear and plain）之文字。資料主體應知悉控管者之身分及其個人資料處理所欲達成之目的。於資料主體並非出於真意；無從自由選擇；無法於不損及其權益之情況下得隨時撤銷其同意；不允許就不同個人資料處理方式分別同意；非屬必要而將契約之履行或服務之提供依存於該同意時，上述情形其同意應推定為不具自主性。此外，「撤回同意」應與「給予同意」一樣容易。

為科學研究目的所為之資料處理，於資料蒐集當時，通常不可能完整指明該處理之目的。因此，當科學研究符合公認之道德標準時，允許資料主體僅就科學研究之特定範圍為同意之表示。資料主體應有機會僅就特定研究範圍或預期目的範圍內之部分研究計畫表示同意。

五、資料主體（當事人）之權利

（一）透明原則（第 12 條至第 14 條）

個人資料之蒐集、利用、處理應向當事人公開，「透明原則」（principle of transparency）要求關於個人資料處理之任何資訊或聯繫，應方便取得、易於理解、且應以清晰易懂之語言為之。透明原則尤其關注於向資料主體公開控管者之身分、其處理資料之目的及其他進一步資訊，用以確保對當事人公正及透明之個人資料處理。當事人應獲告知有關個人資料處理之風險、規範、保護措施及相關權利，如何行使其權利，權利被侵害時之救濟及其方式。

要求控管者必須透過契約要求處理者遵守相關規定，本規則直接要求控管者及（某些情形下的）處理者都必須確實符合相關規定。

（二）接近使用權（第 15 條）

資料主體應有權接近使用（right of access）其被蒐集之個人資料，並得容易的、於合理之時間間隔行使接近使用權，以知悉並確認該處理之合法性。若有可能，控管者應提供得遠端使用之安全系統以提供資料主體直接接近使用權。惟行使該權利不得對他人之權利或自由有不利之影響，包括營業秘密、智慧財產權及軟體著作權等。

為利於資料主體行使本規則之權利，應提供不同之免費管道，包括申請機制及獲得機制。於個人資料係以電子方式處理時，亦應提供電子化申請方式。控管者有義務回應資料主體之請求，不得無故遲延且最遲應於一個月內為之。如因請求之複雜性及數量，必要時得延長兩個月，惟控管者應於收到請求後一個月內通知資料主體該次展期，並說明遲延之原因。控管者不同意該請求時，應附具理由，並敘明向監管機關提出申訴及尋求司法救濟之可能性。

控管者應免費提供所處理個人資料之副本一份[5]，如資料主體要求更多副本，控管者得依行政成本收取合理費用。如資料主體係以電子方式提出請求，除資料主體有不同要求外，該資訊之提供亦應以電子方式為之[6]。

（三）更正權及刪除權（「被遺忘權」）（第 16 條、第 17 條）

資料主體應有修改或刪除其個人資料之權利，以及當資料之保存違反本規則、歐盟法或會員國法時，應有刪除權（right to erasure），或「被遺忘權」（right to be forgotten），即於該個人資料就資料蒐集或處理之目的已無必要時；已拒絕其個人資料之處理時；或已撤回其同意時；或於其個人資料處理違反本規則時，資料主體應有請求不再

---

5 例如：我國唯一跨金融機構間信用資訊機構金融聯合徵信中心（以下簡稱聯徵中心），每年度免費提供社會大眾 1 份含加查其他信用資料之中文信用報告。

6 例如：為提升民眾便利之數位化金融服務，自 104 年 11 月 1 日起，我國年滿 20 歲民眾即可以內政部核發之自然人憑證在聯徵中心網頁線上查閱電子版本個人信用報告，自 106 年 1 月 1 日起，增加加查信用評分項目服務，並將推廣期間免費查閱服務延長至 106 年 12 月 31 日。

處理其個人資料之權利。另方面，資料主體亦應有權請求完整化其有欠缺之個人資料，包括以提供補充說明之方式，即所謂「更正權（right to rectification）」。

為強化網路環境之被遺忘權，刪除權應擴張至「公開個人資訊」之控管者有義務通知「刻正進行個人資料處理」之控管者刪除任何該個人資料之連結、複製或仿製（links, copies or replications）。為確保個人資料未遭留存超過必要期間，控管者應設定個人資料銷毀之期限或定期確認，並採用各種措施更正、刪除或補充不正確之個人資料。

惟本規則亦明定於以下情形不適用刪除權之規定，包括：為行使表意自由及資訊自由者；符合公共利益之職務執行或委託控管者行使公權力所必須者；基於公共衛生領域之公共利益且符合相關規定者；為實現公共利益、科學、歷史研究目的或統計目的且符合相關規定者；及為建立、行使或防禦法律上之請求者。

（四）資料可攜權（第 20 條）

為進一步強化資料主體對自己資料之掌控，當個人資料以自動化手段執行處理時，資料主體應有權以結構的（structured）、廣泛使用的（commonly used）、機器可讀的（machine-readable），及可共同操作的格式（interoperable format）接收其提供予控管者之資料，並有權將之傳送給其他控管者。資料控管者應被鼓勵發展具資料可攜性（data portability）之可共同操作格式。當技術上可行時，資料主體應有權使該個人資料由一控管者直接移轉其個人資料予其他控管者。但資料可攜之權利不得優先於「刪除權」相關規定行使，並且，該權利不適用於符合公共利益而執行職務者，或委託資料控管者行使公權力而為必要處理之情形。

（五）拒絕權（第 21 條）

資料主體得基於與其具體情況有關之理由，隨時拒絕本規則所定[7]

[7] 參照本規則第 6 條第 1 項第 e 款及第 f 款。

關於其個人資料之處理，即所謂拒絕權（right to object）。控管者應不得再處理該個人資料，除非該控管者證明其處理有優先於資料主體權利及自由之法律依據，或為建立、行使或防禦法律上請求所為之者。個人資料處理係為科學或歷史研究目的或統計目的者（參照本規則第 89 條第 1 項），資料主體應有權基於與具體情況有關之理由，拒絕與其有關資料之處理，除非該處理係基於符合公共利益之職務執行之理由而有必要者。

（六）對於自動決策及建檔之相關權利（第 22 條）

資料主體應有權不受自動化決策之拘束（not to be subject to decision），該決策包括對其產生法律效果或類似之重大影響，而係以自動化處理來評估其個人特徵之措施。例如：網路申請貸款之自動拒絕，或不包括任何人為介入之電子化人力招募等。即使為締結或履行資料主體與控管者間之契約所必要，或資料主體已明確同意，資料控管者仍應執行適當措施，以保護資料主體之權利、自由及正當利益。前項措施至少應確保得以部分之人為參與（human intervention）、表達意見（to express his or her point of view）及獲得挑戰該決策（contest the decision）之機會等。

自動化處理包括以任何形式評估個人特徵之「建檔」（profiling）行為，特別是使用個人資料分析或預測資料主體之工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、地點或動向等特徵，而對其產生法律效果或類似之重大影響。控管者應於建檔時使用適當之數學或統計程式、實施科技化且有組織的措施，以確保個人資料得以即時更正，並將錯誤風險最小化。

六、個人資料處理之安全性（第 25 條、第 32 條）

關於個人資料處理之權利及自由之保護，須採取適當之科技化且有組織的措施，亦即，控管者應採取符合「設計（by design）與預設（by default）資料保護原則」之規則與措施。該等措施包括但不限於個人資料處理之最小化（minimising）、盡可能將個人資料

予以假名化（pseudonymising）[8]、個人資料之處理與作用之透明化（transparency）、使資料主體得以監控該資料處理、並使控管者得以創造與提升安全功能等。開發、設計及選擇用以處理個人資料之應用程式、服務與產品時，應將資料保護納入考量，以確保控管者和處理者得以完成其資料保護之義務。尤其在公開招標過程中，前揭「設計與預設資料保護原則」應納入採購規格之重要考量。

考量現有技術、執行成本、處理之本質、範圍、脈絡及目的，與對於當事人權利及自由造成風險之可能性與嚴重性，控管者及處理者應採取適當之科技化且有組織的措施，包括但不限於以下事項：

- 確保系統及服務持續之機密性、完整性、可用性及彈性；
- 在事故發生後及時回復個人資料可用性及可接近性；
- 定期評估、測試、衡量及確保安全措施之有效性。

七、關於兒童之特別保護（第 8 條）

鑑於兒童未能完全知悉其個人資料處理之風險、後果、相關保護措施及權利，兒童之個人資料值得受特別保護，尤其在為行銷或建立使用者檔案之目的。任何提供予兒童之資訊及溝通，應採用兒童易於理解且清晰簡易之語言。

資料主體同意之要件適用於直接向兒童提供資訊社會服務之情形，如兒童年滿 16 歲，兒童之個人資料處理應屬合法；如該兒童未滿 16 歲，僅限於父母或監護人授權或同意之範圍內，該等處理始為合法[9]。惟直接向兒童提供預防性（preventive）或諮詢性（counselling）

---

[8] 依本規則第 4 條之定義，「假名化」（pseudonymisation）係指處理個人資料，使其在不使用其他附加資訊時，無法識別出特定之資料主體，且該附加資料已被分開存放，並以技術及措施確保該個人資料無法識別當事人。與我國個人資料保護法所稱之「去識別化」（de-identification）相近。

[9] 本規則第 8 條「涉及資訊社會服務適用兒童同意之條件（Conditions applicable to child's consent in relation to information society services）」另規定，歐盟各會員國得以國內法另定較低之年齡，但不得低於 13 歲。另，關於兒童個人資料處理之合法性，不影響一般契約法（例如與兒童有關之契約）之成立或有效性。

之服務時，無須得其父母或監護人之同意。資料主體於兒童時期所為之同意，應推定為未能完整理解該處理所存在之風險，其後希望移除其個人資料（特別是網路上資料）時，得依本規則行使相關權利。

八、特種個資之處理（第 9 條）

揭露種族、政治意見、宗教或哲學信仰之個人資料、基因資料、用以識別自然人之生物特徵識別資料、涉及前科及犯罪之個人資料、與健康相關或性生活或性傾向等有關個人資料之處理，原則上應予以禁止。但依本規則或會員國法律規定，資料主體已明確同意或已自行公開；為履行義務及行使控管者特定權利之目的；為行使法律上請求或司法機關執行司法權；或為保障資料主體之基本權及利益而有必要之處理等，不在此限[10]。

九、個人資料保護影響評估（第 35 條）

就個人資料之處理可能造成當事人之權利或自由有高度風險之情形，控管者應於處理前執行資料保護影響評估（data protection impact assessment），以衡量風險的來源、本質、特殊性與嚴重性，尤其應包括預計用以降低風險及確保個人資料保護的措施與機制。為證明個人資料之處理符合本規則，在決定有關資料處理之適當措施時，前揭評估之結果應納入考量。

資料保護影響評估尤其應適用於處理地區性、國家或超國家層級可觀數量之個人資料，例如：就當事人之個人特徵為體系性及密集性之評估、大規模使用新技術建檔資料，或透過特殊類型之個人資料、生物資料、前科及犯罪資料或相關安全措施等之資料處理。資料保護影響評估在大規模監控公共場合（monitoring publicly accessible areas on a large scale）亦有必要，特別是運用光學電子裝置，或主管機關認為有可能對資料主體之權利與自由造成高度風險之任何其他情形。

---

[10] 詳細之排除要件規定，請詳本規則第 9 條「特殊類型之個人資料處理（Proces sing of special categories of personal data）」第 2 項各款規定。

十、個人資料之國際傳輸（第 44 條、第 45 條）

為了增進國際貿易與國際合作，個人資料之國際傳輸有其必要，但資料於國際流通之增加已然帶來了新的挑戰與有關個人資料保護之課題。在任何情況下，向第三國或國際組織之個人資料移轉僅得於完全遵循本規則之前提下執行，唯有當控管者或處理者已遵守本規則所定關於個人資料移轉至第三國或國際組織之規範，且受本規則所定其他條款之拘束時，個人資料之移轉始得為之。第三國應確保有效而獨立之資料保護監督機制（effective independent data protection supervision）、對人權、法治與自由之基本尊重，且應提供資料主體有效且可實現的權利及有效的行政與司法救濟。

十一、資料保護官（員）（第 37 條至第 39 條）

除法院行使司法權外，由公務機關或機構執行個人資料處理處理時；控管者或處理者需要定期且系統性地大規模監控（regular and systematic monitoring）資料主體時；大規模處理特殊類型個人資料或與前科及犯罪相關之個人資料時；或歐盟或會員國法有明確要求時，應指定具資料保護法律與實踐之專業知識的資料保護官／資料保護員（data protection officer）。

資料保護官直接向處理或管理者之最高管理階層報告，並應確保其免於任何有關執行職務之指令，且不得因執行職務被解任或處罰。控管者及處理者應確保資料保護官適當且及時的，涉入所有有關個人資料保護之業務。

十二、資料保護認證及資料保護標章（誌）（第 42 條）

為提升本規則之透明度與對本規則之遵循，鼓勵認證機制（certification mechanisms）與資料保護標章及標誌（data protection seals and marks）之建立，以證明控管者及處理者之處理活動遵守本規則，並使資料主體得以快速評估相關產品及服務之資料保護程度。相關認證及標章（誌）均須定期接受評估及更新。

十三、歐洲個人資料保護委員會（第 68 條）

為促進本規則之適用，歐盟設立有法人格地位之獨立委員會（Board），取代歐盟指令 95/46/EC 所設立之個人資料處理保護工作小組（Working Party）。其組成應包括各會員國監管機關及歐盟資料保護監管機關之首長或其相對應之代表。歐盟執行委員會應參與委員會之活動，但無表決權；歐盟資料保護監管機關應有特別表決權（specific voting right）。

十四、個人資料侵害之通報及損害賠償（第 33 條、第 82 條）

一旦控管者發現個人資料侵害已然發生，應即向監管機關通報，不得無故遲延。若可能，應於發現後 72 小時內通報，控管者如證明依歸責原則，該個人資料之侵害不可能造成當事人權利與自由的風險者，不在此限。當該通知無法於 72 小時內到達時，遲延之原因應與通知一併提交，並且不得更進一步遲延。

因違反本規則而遭受物質上或非物質上之損害時，任何人應有權自控管者或處理者就其損害獲得賠償。惟如控管者或處理者可證明其對於損害之造成不可歸責時，得免除賠償責任。

十五、行政罰鍰之裁處（第 83 條）

違反本規則有關控管者及處理者之義務、認證機構之義務或監管機構之義務者，最高處以一千萬歐元之行政罰鍰；如為企業，最高處以前一會計年度全球年營業額之百分之二，並以較高者為準。

違反有關資料處理之基本原則、個人資料國際傳輸之規定、侵害本規則所定資料主體之權利、或違反依照本規則通過之會員國法律所定之任何義務者，最高處以二千萬歐元之行政罰鍰；如為企業，最高處以前一會計年度全球年營業額之百分之四，並以較高者為準。鉅額之法定裁罰上限及有效之計算基準（跨國企業之全球年營業額），對違法者嚇阻力十足。

肆、結語

歐洲共同市場的運作除促進社會與經濟之融合，亦增加個人資料之跨境流通，個人資料在機關與私人間，包含跨歐盟各國間之個人、組織及企業間之資訊交換規模大幅增加，特別是在涉及網路活動時。科技的快速及全球化發展，對個人資料保護也帶來新的挑戰，蒐集、處理及共享個人資料之規模已顯著提升，並更加公開化與國際化。為確保個人資料之全面保護，確實應賦予當事人對其個人資料更高度且更全面的保護與控制權。本文謹就本次歐盟「個人資料保護規則」大幅擴充之規範內容（包括長達 173 點之法規前言及共 11 章、99 條之法規本文）作初步之導讀及綱要性介紹，期能拋磚引玉，並將此一劃時代的重要法典中譯並引介給我國政府相關部門、產業及學術研究等各界卓參。

歐盟新規：個人資料保護規則－數位防護的新縱深

林思惟 / 金融聯合徵信中心 研究部經理

由於歐盟會員國在個人資料保護相關法律缺乏一致性的架構，以及近年來雲端計算、行動互聯網、大數據等資訊科技的快速發展，對個人資料保護帶來新的議題與挑戰，歐盟對 1995 年立法「資料保護綱領（EU Directive 95/46/EC: the Data Protection Directive）」進行大刀闊斧的改革。歐盟執委會自 2012 年 1 月提出資料保護改革草案以來，其嚴苛的規範撼動資訊科技界的巨擘於歐盟經營的根基，紛紛投入龐大的資源向歐盟當局進行遊說，歐洲議會共計收到四千多份相關修正意見，經過 4 年多的討論，歐洲議會終於在 2016 年 4 月 27 日通過歐盟規則 2016/679，亦即「個人資料保護規則（the EU General Data Protection Regulation，以下簡稱 GDPR）」，此規則自 2016 年 5 月 24 日起生效，並取代歐盟 1995 年的「資料保護綱領」。新法規定 2 年過渡期，直到歐盟各成員國均實施 GDPR，才自 2018 年 5 月 25 日起全面施行新法。

GDPR 不僅適用於歐盟地區註冊的企業，非屬歐盟企業組織但在歐盟境內營運，蒐集、處理或利用歐盟人民的個人資料者，須適用本法。此外，GDPR 除了提升個資保護強度，且大幅提高了罰款金額上限法規，最高可處罰鍰 2 千萬歐元或年度全球總營業額 4% 的金額。由於 GDPR 與信用報告機構之營運關係密切，歐盟消費者信用資訊業協會（Association of Consumer Credit Information Suppliers，簡稱 ACCIS）[1] 亦投入相當人力與資源，針對信用報告產業的特殊議題，積

[1] 消費者信用資訊業協會（ACCIS），成立於西元 1990 年，原始註冊地為愛爾蘭首府都柏林，成立宗旨為結合歐盟地區之消費者信用報告機構力量，設定主要共同利益

極進行遊說。

一、GDPR 修訂重點

（一）提升法律位階：由 Directive 提升為 Regulation

歐盟在 1995 年制定的資料保護綱領（Directive）僅係依歐盟地區廣泛共通的法律框架與指導原則，歐盟各會員國可依各國之情況，制定各國的資料保護之法規與措施，也因而造成了歐盟地區各會員國對資料保護之程度仍存在極大的差異。而 GDPR 之法律位階屬於 Regulation 層級，已經過歐洲議會（European Parliament）與歐盟理事會（European Council）的議決，將直接適用於歐盟各會員國，而不再需要透過會員國國內法的轉換，2018 年 5 月直接適用各成員國，這將徹底解決成員國之間的法律制度差異問題，此一改變將降低跨國企業的法規遵循成本，且僅需接受單一的監理機構之監管（One stop shop）。歐盟亦將成立統一之「歐盟資料保護委員會（European Data Protection Board，EDPB）」，藉由發佈意見（opinions）、準則（guidance）、建議等（recommendations），維持歐盟地區資料保護制度之跨國一致性。

（二）擴大適用範圍 Expanded territorial scope

1995 年資料保護綱領適用屬地原則，如果企業提供跨境服務，但並未於歐盟地區設立，則可規避歐盟法律。在 GDPR 的規範，即使資

與優先順序，於整體歐盟層次與各國層次，積極影響並遊說有利於會員經營之法制環境，使會員在國內外持續發展業務；並設定重要議題，以信用報告機構之利益與觀點，透過各項跨國合作之專案研究，提供行政部門在制定管制信用報告機構之相關政策時參考。

2006 年該協會改制，在比利時登記為國際性非營利組織，總部設於比利時布魯塞爾。目前該組織正式會員有 42 家位於歐盟地區之信用報告機構（分布於 28 個國家），另有 6 個非正式之非歐盟會員（Associate Member），分別為：台灣（金融聯合徵信中心）、中國大陸（中國人民銀行徵信中心）、墨西哥（Buro de Credito TransUnion de Mexico SA SIC）、泰國（National Credit Bureau Company）、美國（MicroBilt Corporation）、荷屬加勒比海群島（Caribbean Credit Bureau N.V.）。今年起，ACCIS 增加另一類會員：聯盟會員（Affiliate Member），目前僅有 FICO 公司一家。

料控制者於歐盟境內沒有設立機構，但其在跨境提供商品或服務的過程中，蒐集處理歐盟居民個人資料，則應當適用 GDPR 之規範，並需要在歐盟境內指派特定代表負責法令遵循事宜。這一規定將影響大多數資訊科技巨擘（如微軟、Google、Facebook 等）。

（三）企業必須設置「資料保護長 Data protection officer，DPO」

為確保企業（條文所稱「資料控制者 data controller」或「資料處理者 data processor」）之有效遵循法規，GDPR 歐盟要求如果企業員工超過 250 人，且核心業務涉及到對歐盟居民的資料處理，大型企業必須設立資料保護長（DPO）。此一職位並必須有效依法履行職責，若企業違反 GDPR 之規範，DPO 將被追究法律責任。

（四）資料蒐集與處理須取得明確有效同意

1995 年資料保護綱領並沒有規定同意應當是「明示同意」還是「默認同意」。GDPR 規範企業負有保護資訊蒐集更加透明化的責任，所以企業必須獲得用戶之同意，該同意必須由資料當事人自主的授予（freely given）、具體（specific）、知情（informed）以及明確（unambiguous），方能取得並處理個人資料，尤其針對敏感性資料（sensitive data）更必須明確清楚（explicit），企業必須能夠證明已取得資料當事人之同意，當事人保持沉默、未表示意見或無作為情形，皆不構成前述「同意」，兒童或青少年個資之取得及處理，須事先獲得父母或監護人同意。既有同意若符合 GDPR 的要求，則仍然有效。且企業必須提供資料當事人以簡單的方式，撤回授權企業取得與處理個人資料的同意，用戶個人資料被取得後將被用在什麼用途，也必須清楚直白地說明陳述。

（五）個人資料可攜權 Data portability

GDPR 除了規範企業，也使歐盟公民能對自己的個資擁有更大的操控權，包括「資料可攜權」，也就是在不同服務間移動個資的權利，用戶可以將其個人資料以及其他相關資料從一個網路服務供應商（ISP）轉移至另外一個 ISP（例如將所有連絡人資料和郵件從 Google

移動到 Yahoo）。

（六）個人資料外洩通報 Data breach notification

GDPR 規定，企業（含資料控制者或資料處理者）若發生個人資料外洩事件（data breaches），必須於知悉後 72 小內通報其資料保護主管機關（Data Protection Authority），且若對資料當事人之權益有重大危害之虞，雖未明確規範期限，惟亦應及時（without undue delay）通知資料當事人。

（七）IT 系統之資料保護設計 Data protection by design and by default

企業為了提供產品和服務，必須蒐集與處理個人資料，除須符合明確同意等規範外，亦必須遵循個人資料蒐集最小原則（data minimization），GDPR 亦將「個人資料」擴大解釋為涵蓋可直接或間接過濾出特定對象資訊之資料類型，例如網路瀏覽器 Cookies、網路 IP 位址或足以辨識特定個人身分或性別之基因、生物特徵或醫療資料等。且 GDPR 引入「資料保護設計（Data protection by design and by default）」制度，亦即企業於新資訊系統建置與設計時，即應將資料保護之設計納入考量，亦即各類產品或和業務線，在業務設計的最初階段，就需要與 IT 廠商充分協商，並通過技術、合約、管理等措施落實遵循 GDPR 之要求。

（八）被遺忘權 Right to be forgotten

被遺忘權（Right to be forgotten）是新的保護規則的另一大重點。增加被遺忘權利的目的，旨在賦予個人可更有效的控制其個人資料。在 1995 年資料保護綱領即規範了資料當事人除可要求查閱、複製資料控制者所擁有的個人資料，若該資料有不正確、不完整時，可要求更正、刪除或封鎖（rectification, erasure or blocking），GDPR 更進一步提出被遺忘權的規範，亦即認為除了資料不正確或不完整外，有其他理由時（例如：非法處理個人資料、資料當事人同意已經撤回等六種情況），個人均可要求刪除控制者所掌控之個人資訊。在此之前，歐洲法院已有判例裁定個人可以要求搜尋引擎（Google）從包括「不相

關」或「過期」的個人資訊結果中移除連結。

（九）反對權（Right to object）

在 GDPR，個人反對權（Right to object）與「被遺忘權」，乃是不同之權利。個人反對權係資料當事人有權，在特定情況下，反對資料之處理，除非資料控制者證明處理該資料有重大正當理由，勝過資料當事人之基本權利與自由。當資料當事人提出反對時，資料控制者應立即停止處理該個人資料。反對權亦適用於以大量個人資料所自動化產生之「描繪（profiling）」活動，亦即，資料當事人有權瞭解一項特定服務是如何做出特定決策的，此一規範將對以大數據為基礎，運用機器學習、人工智慧技術進行資料分析與研判的服務（例如，Facebook 透過演算法提供客製化資訊內容），將形成重大挑戰，畢竟類似「黑盒子」的機器學習技術很難適用「反對權」。

（十）對自動化決策之限制

GDPR 對於以大量個人資料所自動化產生之「描繪（profiling）」進而進行決策有諸多規範。自動化決策之概念係指：以自動化方式處理個人資料的分析與預測活動，而產生對資料當事人包括工作表現、經濟狀況、位置、健康狀況、個人偏好，可信賴度或者行為表現等之判定。GDPR 規定：「描繪（profiling）」必須具有法定依據或者獲得用戶明確同意；用戶必須是在充分知情下做出同意授權；不得針對敏感議題（例如：種族、政治立場、宗教信仰、性取向等）進行。

（十一）資料保護影響評估（Data Protection Impact Assessments，DPIA）

GDPR 要求企業必須進行「資料保護影響評估（Data Protection Impact Assessments，DPIA）」，用以辨識業務活動中涉及個人隱私權利的風險，並加以衡量、管理與因應，並於蒐集與處理個人資料前，評估該等風險與業務活動必要性與對稱性。DPIA 與許多企業已實施之「隱私影響評估（Privacy Impact Assessments，PIAs」類似，惟 PIAs 並無明確的規範與定義，DPIA 則強化了其內涵與一致性。

（十二）大幅提高罰則金額

GDPR 大幅提高違規罰款的金額，依違反情節給予不同程度的罰款，例如：沒有合法理由，拒絕用戶刪除個人數據請求，沒有建立企業對用戶數據保護的文件化管理，最高將被處以 1000 萬歐元或全球營業總額的 2% 的罰款；第三類違規行為：非法處理個人數據；沒有合法理由，拒絕用戶關於停止處理個人數據的請求；在數據洩露事故發生之後，沒有及時通知監管機構；沒有執行隱私風險評估；沒有任命數據保護官，違法向第三國傳輸個人數據；最高將被處以 2000 萬歐元或全球營業總額 4% 的罰款。

二、ACCIS 對 GDPR 之關注焦點及 GDPR 立法結果

GDPR 與信用報告機構之營運關係密切，自 GDPR 於 2012 年啟動修法工程起，ACCIS 即投入相當人力與資源，針對信用報告產業的特殊議題，積極進行遊說。並對業界重大議題，以 ACCIS 名義，提出說帖（Response to the proposal for a General Data Protection Regulation– Perspective of Credit Reporting Agencies），並積極進行遊說，長達四年的努力，成果大致符合 ACCIS 的預期。其重點如下：

（一）企業之「合法利益」仍列為得以處理個人資料之要件之一

1995 年制定的資料保護綱領（Directive）第 7 條（Article 7）規範了企業得以處理個人資料的 6 項要件，其中（f）項允許在企業追求其「合法利益（legitimate interests）」之範圍內，可以作為處理個人資料之依據。在 GDPR 的立法過程中，此一規定引發相當程度的討論，許多消費者保護團體主張企業「合法利益（legitimate interests）」定義與界線並不容易認定，企業可能過分主張其「合法利益」而犧牲了資料當事人的權利。ACCIS 針對此一議題，積極主張應予保留。GDPR 最終結果：未將「合法利益」刪除。

（二）對「合法利益」之反對權（Right to Object）之限縮

GDPR 立法階段曾將「合法利益」列為資料當事人行使「反對權」的重點，並設計極為嚴苛，對信用報告機構業者極為不利的規範（例

如：一經資料當事人反對，信用報告機構即刪除，或應停止對其個人資料的處理與利用）。GDPR 最終結果：未將嚴苛之「反對權」行使規範納入。

（三）對自動化決策之「描繪（profiling）」活動不強制人工介入

GDPR 對於以大量個人資料所自動化產生之「描繪（profiling）」有相當程度的疑慮，而信用報告機構所提供之「信用評分」服務類似於 profiling 之概念，若所有信用評分結果都必須經人工審視，在實務上，對十分重視即時回應的信用交易十分不利。GDPR 最終結果：未將人工介入之強制性要求納入。

（四）移除對敏感性資料的限制使用

GDPR 原有意定義特殊類別的個人資料（special categories of personal data），諸如：性別、法院或行政判決等，並限制不得處理使用。由於法院判決與行政裁罰資料長久以來為信用報告機構所蒐集與提供，且該項資訊對於金融機構避免消費者過度負債（over-indebtedness）有極大之助益。GDPR 最終結果：未限制法院判決與行政裁罰資料之使用。

三、GDPR 對信用報告機構之影響

GDPR 除加強個人資料保護的強度之外，亦使歐盟 28 成員國資料保護規定獲得統一，可望減少跨國企業在遵守各成員國資料保護規定上之不便情形，由於其適用範圍對象涵蓋非歐盟國家之企業，在立法階段，即引發全球性資訊巨擘與跨國大企業的高度關注，藉由商業全球化、網路化的發展，個人資料的跨國蒐集、處理與傳遞在所難免，而 GDPR 的實施，首波衝擊將影響與歐盟市場往來密切的商業活動（主要為美國企業）帶來巨大的衝擊，進而擴及至全球其他與歐盟有經貿往來之區域。

以信用報告機構經營的角度而言，雖然 ACCIS 在 GDPR 立法上的遊說成果，大致保住了既有的經營基礎，但 GDPR 於 2018 年的正式實施，仍對信用報告業者帶來許多不確定性的因素。

（一）各會員國資料保護程度的差異有待解決

GDPR 跨國一致性的規範，將凸顯各國現有資料保護程度的差異，而歐盟層級的「歐盟資料保護委員會（European Data Protection Board，EDPB）」，亦將徵詢各國的實務，藉由發佈意見與準則（opinions and guidance），補充 GDPR 未明確規範的空間，以利 GDPR 跨國一致性的執行。

（二）信用報告機構之可歸責性（Accountability）增加

在 GDPR 的規範下，信用報告機構不論擔任資料「控制者（controller）」或是資料「處理者（processor）」的角色，其「可歸責性」將更為清楚，違反規定所付出的代價將更高，因此信用報告機構應建立遵循 GDPR 要求之內部健全的管理與控制機制，並證明該機制可有效運作。

（三）資料當事人權利（Data Subject Rights）之行使

GDPR 新增了許多保護資料當事人權益的規範，例如：個人資料之刪除與更正；資料可攜權 Data portability（企業必須免費提供完整的電子檔案資料）；個人資料處理的通知等，在信用報告機構的現行運作中，皆已有一定遵循機制，例如：接受資料當事人對信用資料的爭議及後續處理；資料揭露期限的訂定；（免費）信用報告的提供等，惟是否符合 GDPR 之要求，信用報告機構業者應進行盤點與比對，若有不足之處，擬訂改善計畫並與監理機關密切溝通。

（四）只是開始，不是結束

在「合法利益」、「被遺忘權」、「反對權」、「特殊類別的個人資料」等議題，雖然信用報告機構業者在 GDPR 的立法中占了上風，但該等議題已引發各界的關注，後續可預期將有更多消費者保護團體針對此等權利提出「是否濫用」的質疑，「歐盟資料保護委員會」亦將密切注意其發展，任何一個會員國資料保護主管機關（Data Protection Authority）所作的決定，都可能影響整體歐盟，信用報告機構宜小心應對。

四、GDPR 對我國信用報告機構發展之啟發

個人資料保護的立法概念，一般偏重於保護社會大眾與相對具有權力與經濟優勢之公務機關或私人企業往來時，其個人資料之合理運用與隱私權利的適度保障。若將此種消費者保護概念，應用於民眾與金融機構往來希望能以合理的條件取得所需信用的情境中，則產生諸多值得特別深入探討的面向。

在信用交易市場中，「信用需求者」與「信用供給者」之間存在之資訊不對稱，是阻礙信用交易效率進行的最大障礙，「信用需求者」必須提供足以供「信用供給者」評估信用風險所需之資料，以換取從「信用供給者」取得信用的機會。

當「信用供給者」為金融機構時，由於金融機構授予「信用需求者」之資金係來自於社會大眾的存款，金融監理機關基於金融穩定的考量，對金融機構的信用風險管理會訂定較高的標準，並以監理手段要求銀行確實遵循。除此之外，監理機關亦可能透過法制的設計與安排，設立專責跨機構蒐集與提供信用資料的「信用報告機構」，以提升銀行對「信用需求者」信用資訊可蒐集的廣度與深度；於此情境下，有信用需求之個人必須 牲較多的個人資料保護程度，甚至必須放棄某種程度之「被遺忘權」，以換取使用社會大眾存款的機會，以及整體金融信用體系的健全發展，進而建立公平合理的信用市場紀律。

財團法人金融聯合徵信中心（以下簡稱聯徵中心）即循上述概念，在「銀行法」、「銀行間徵信資料處理交換服務事業許可及管理辦法」的法規安排下所設立之非營利性財團法人機構。聯徵中心採「會員制」管理，透過「會員規約」（目前會員僅限經許可設立之金融機構，包括：銀行、信用合作社、票券金融公司、證券金融公司、農會信用部、漁會信用部、信用卡公司、經營授信業務之保險公司等），經營會員機構信用資訊之蒐集、處理與交換之特許業務，以解決「信用需求者」與「信用供給者」之間存在之資訊不對稱的癥結，經逾四十年的運作，個人資料保護與授信管理目的個人資料分享，大致維持均衡與穩健。

如今，隨著數位科技的發展，「普惠金融（financial inclusion）」得以快速發展並有效實現，模糊與動搖了原本牢固封閉的金融領域。「普惠金融」的目標為讓經濟地位弱勢者（即：無法獲得金融服務者 unbanked，以及金融服務不足者 underbanked），藉由取得與享用完整的金融服務（存款、匯款、貸款、保險、理財等現代經濟活動所必須之服務），達成脫離貧窮的實質目的，其方式為透過金融科技大幅降低提供金融服務成本與門檻，提升對經濟活動的相對弱勢者金融服務的深度與廣度，而不論該種金融服務之提供係來自於傳統金融機構，或來自於非金融機構的科技業者，數位化個人資料廣泛的蒐集處理與利用皆為必要的途徑，而在現今的資訊科技環境下，個人資料之保護運用，亦變得十分複雜與棘手，此即歐盟訂定 GDPR 的主要背景。

傳統信用報告機構所蒐集、使用之信用資料，係以資料來源清楚可信、資料定義明確的結構化資料為主；而新型態信用報告服務提供者所使用之數位資料，其資料範圍廣泛、資料面向多元、資料即時且動態，加以處理大量資料之分析方法之日益成熟，藉由多維度資訊彼此的關聯性來描繪資料主體之信用狀況，已實質改變傳統信用分析之既有框架。

但新型態信用報告服務提供者所大量使用之數位資料，除了須面臨資料缺乏一致性客觀定義、資料的變動並未經嚴謹的更新與更正程序、資料操弄與作假疑慮及資料與信用良好與否的相關性難以驗證等先天性課題外；在應用大數據資料之情形下，若資料當事人引用前述歐盟 GDPR 行使「被遺忘權」或「反對權」，或質疑大數據可能帶來的「資料獨裁問題」（意指：在大數據的環境下，透過人工智慧技術，根據數據分析將人群進行分類與標籤化），亦會產生 GDPR 所至為關切的以資料進行被分析對象的「描繪」與資料當事人之「反對權」議題。

在數位資訊科技一日千里的高度動態環境中，「資料保護」與「普惠金融」兩種概念的相互碰撞，激起了跨領域之監管議題，政府不同

部門間對於數位科技所帶來全新的便利與威脅，雖必然存在不同立場的觀點，但監管者都必須強化對數位科技的認識，在一定程度的專業理解下，進行跨部門的溝通與論證，甚至應用數位科技強化監管的效率與效能，亦即「法遵科技（RegTech）」的新概念。除此之外，任何監管措施實施之前，亦應充分與被監管者進行有效的溝通，在可控制的範圍內進行試作，透過實際操作，確實瞭解科技運用的潛在風險與威脅，並以風險為基礎（risk-based），設計有效且精準法規遵循與金融監理措施，實質降低被監理者法規遵循之負擔，此即為「監理沙盒（Regulatory Sandbox）」的概念。

雖然 GDPR 的實施及歐盟地區信用報告機構的發展對於聯徵中心無明顯或立即的影響，惟從 GDPR 的修訂或觀察目前影響全球或歐盟信用報告業發展的重大趨勢，皆可發現資訊科技發展所帶動的數位化、網路化、行動化、雲端化所產生之個人資料保護與使用議題、資訊跨國傳遞與金融跨國監理議題等，早已成為信用報告業者之關注焦點；聯徵中心仍應未雨綢繆，瞭解國際趨勢，針對個人資料保護等相關議題預作研議，俾於未來議題形成與討論階段，以公益性信用報告機構之立場，向政策制定部門提出妥適之建議，以當事人權益為優先考量之前提下，兼顧我國信用報告機構之健全發展。

REGULATIONS

規則

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)

於 2016 年 4 月 27 日
歐洲議會及歐盟理事會
為保護自然人(*)之個人資料處理與自由流通
制定歐盟規則第 2016/679 號（個人資料保護規則）
取代第 95/46/EC 號歐盟指令

(Text with EEA relevance)

（本文本適用於歐洲經濟區）

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

* 譯者註：原文多處使用 the protection of natural persons with regard to the processing of their personal data 一語，如加以直譯，固指自然人之個人資料保護，惟參照我國個人資料保護法之法規名稱及其第 2 條第 9 款將個人資料之本人稱為當事人的規定，以下就 natural personal 依其脈絡不特別翻譯，或翻譯為當事人或個人。

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3],

Whereas:

歐盟所屬歐洲議會及歐盟理事會，根據

歐洲聯盟運作條約，特別是第 16 條規定，

歐盟執行委員會之提案，

將立法草案交由會員國國會後，根據

歐盟經濟暨社會委員會之意見[1]，

歐洲區域委員會之意見[2]，

依據通常的立法程序[3]，

鑑於：

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union

---

1 OJ C 229, 31.7.2012, p. 90.
官方公報 C 類第 229 期，2012 年 7 月 31 日，第 90 頁。

2 OJ C 391, 18.12.2012, p. 127.
官方公報 C 類第 391 期，2012 年 12 月 18 日，第 127 頁。

3 Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
歐洲議會於 2014 年 3 月 12 日所持立場（尚未刊載於官方公報）及理事會於 2016 年 4 月 8 日一讀所持立場（尚未刊載於官方公報）。歐洲議會於 2016 年 4 月 14 日所持立場。

(TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(1) 個人資料處理之保護乃基本權。歐洲聯盟基本權利憲章（下稱憲章）第 8 條第 1 項及歐洲聯盟運作條約（即 TFEU）第 16 條第 1 項規定，任何人有保護其個人資料之權利。

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(2) 個人資料處理之保護原則與規則為應尊重其基本權及自由，尤其是其保護個人資料之權利，而不問其國籍或住居所。本規則旨在實現一個自由、安全及公義之經濟聯盟，促進經濟與社會進步，強化及融合歐洲市場之經濟，並追求個人之福祉。

(3) Directive 95/46/EC of the European Parliament and of the Council[4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(3) 歐洲議會及歐盟理事會[4]之歐盟指令第 95/46/EC 號，旨在調和各會員國間關於個人資料處理活動所涉及之個人基本權及自由之保護，並確保會員國間個人資料之自由流通。

---

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
歐洲議會及歐盟理事會於 1995 年 10 月 24 日為保護個人有關個人資料處理及自由流通制定歐盟指令第 95/46/EC 號（官方公報 L 類第 281 期，1995 年 11 月 23 日，第 31 頁）。

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(4) 個人資料之處理應為造福人類所設。個人資料保護之權利並非絕對權；必須考慮到其在社會上之作用，依照比例原則，平衡兼顧其他基本權。本規則尊重全部基本權，並遵守條約明訂受憲章所保障之自由與原則，特別是尊重私人及家庭生活、住家及通訊、個人資料保護、思想、良心及宗教自由、言論及資訊自由、營業自由、有效救濟及公正審判之權利與文化、宗教及語言之多元性。

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(5) 歐洲市場的運作所造成社會與經濟之融合已大幅增加個人資料之跨境流通。個人資料在機關與私人間，包括橫跨歐盟之個人、組織及企業間之交換已然增加。歐盟法律要求會員國之機關應

合作並交換個人資料，以便其能夠在其他會員國境內以機關身分履行職責或執行任務。

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(6) 快速的科技發展及全球化對於個人資料之保護帶來了新的挑戰。蒐集與共享個人資料之規模已顯著提升。科技使私人企業及公務機關得以前所未見之規模利用個人資料開展活動。當事人日益使其個人資料公開化及國際化。科技改變了經濟與社會生活，且應進一步促進個人資料在歐盟內自由流通及在第三國及國際組織之移轉，並同時確保個人資料之高度保護。

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(7) 鑑於建立足使數位經濟在歐洲市場發展之信任有其重要性，實需在歐盟內建構強力且更一致之資料保護框架，並落實執法。當事人應有其個人資料之控制權。關於當事人、業者及公務機關方面之法及實務之安定性均應予提昇。

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(8) 凡本規則明定以會員國法律來規範或限制之規定者，於為達一致所必要，且為使內國規定為受規範者可得理解之範圍內，會員國得將本規則之內容整合到其內國法規定。

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(9) 歐盟指令第 95/46/EC 號之宗旨與原則仍屬健全，惟其已無法阻止歐盟內資料保護之實行斷層、法的不確定性或對於個人資料保護具有顯著風險之普遍大眾認知，特別是涉及網路活動時。各會員國對於當事人權利及自由在保護程度上之差異，特別是在會員國境內之個人資料處理而言，個人資料保護之權利落差可能阻止了個人資料在歐盟內之自由流動。上述差異可能因此阻礙歐盟對於經濟活動之執行、造成不當競爭及妨礙機關根據

歐盟法所應履行之職責。上述保護程度上之差異係源自於歐盟指令第 95/46/ EC 號在執行及實務應用上之良莠不齊。

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(10) 為確保對當事人維持一致且高度之保護，並排除個人資料在歐盟間流通之阻礙，關於資料處理之個人權利及自由之保護程度應於全體會員國間一體適用。關於保護個人資料處理之個人基本權及自由所涉及之規範應確保得以持續劃一地在歐盟中加以執行。關於個人資料處理，為遵守法定義務、符合公共利益執行職務或委託資料控管者行使公權力，會員國應被允許維持或

採用其內國法規定，以進一步具體化本規則所定規範之適用。與為實行第 95/46/EC 號歐盟指令關於資料保護普遍及水平適用之法律相結合，會員國就幾個領域之特定部門法尚需更多具體化之規定。本規則亦提供會員國變通條款以具體化其規範，包括對特殊類型之個人資料（「敏感資料」）之處理。在此範圍內，本規則並未排斥會員國法律依其國情為特定資料處理情形作出規定，包括更精準地決定在何種特定情況所為之個人資料處理係屬合法。

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(11) 歐盟境內對於個人資料之有效防護需要加強，且需要詳細列明資料主體之權利及個人資料處理者與其決定者之義務，以及為監測及確保個人資料保護符合法規之相當權力與對於會員國內所生侵權行為之相當制裁。

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(12) 歐洲聯盟運作條約第 16 條第 2 項授權歐洲議會及歐盟理事會擬定關於保護個人資料處理及自由流通之規則。

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and

to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC[5].

(13) 為確保歐盟境內對於當事人之保護程度一致，並防止差異性阻礙了歐洲市場內個人資訊的自由流通，本規則有必要為業者（包括微型及中小型企業）提供具法律確定性及透明度之規範，且為個人提供在全部會員國境內對於控管者與處理者有相同程度之法律上可執行的權利、義務及責任，以確保不同會員國之監管機關對於個人資料處理之一致監控、等效制裁及有效合作。為使歐洲市場正常運作，個人資料於歐盟境內之自由流通不得

[5] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).
2003 年 5 月 6 日歐盟執行委員會關於微型及中小型企業定義之建議（根據文件 C（2003）1422 通報）（官方公報 L 類，第 124 期，2003 年 5 月 20 日，第 36 頁）。

以保護個人資料處理為由而予以限制或禁止。慮及微型及中小型企業之具體情況，本規則就員工人數少於 250 人之組織在記錄保存方面定有排除適用條款。此外，本規則鼓勵歐盟組織及機構以及會員國及其監管機關，考量微型及中小型企業在適用本規則時之具體需求。所謂微型及中小型企業之定義，應依據執委會 2003 年公佈之第 2003/361/EC 號建議書附件第 2 條規定定之 [5]。

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(14) 本規則所保護者，係不論當事人之國籍或住居所，凡涉及其個人資料之處理均屬之。本規則並未涵蓋法人及具法人資格之特定事業的個人資料處理（包括法人名稱、設立形式及其聯繫方式）。

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(15) 為防止產生規避之嚴重風險，當事人之保護應屬技術中立，且不應依賴於已使用之技術。如檔案系統中已包含或旨在包含個人資料者，當事人之保護均有適用，而不問其係透過自動化及

手動化方式處理之個人資料。未依照特定標準建構之檔案或檔卷及其等封面則不在本規則之適用範圍內。

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(16) 本規則並不適用於個人資料涉及在歐盟法外治權領域活動（例如國家安全之活動）所生之基本權及自由保護議題或其自由流通。本規則不適用於會員國在進行歐盟共同外交及安全政策活動中所為之個人資料處理。

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council[6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(17) 歐洲議會及歐盟理事會[6]所訂定 45/2001 號規則適用於歐盟當

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
歐洲議會及歐盟理事會於 2000 年 12 月 18 日為保護個人有關共同體組織及機構處理個人資料及自由流通制定歐盟規則第 45/2001 號（官方公報 L 類第 8 期，2001 年 12 月 1 日，第 1 頁）。

局、機構、辦事處及局處所為之個人資料處理。歐盟規則第45/2001 號及其他涉及個人資料處理之歐盟法案應依本規則所建立之原則與規定加以調整修正，並按本規則予以解釋適用。為在歐盟內建構強力且一致之資料保護框架，歐盟規則第 45/2001 號應隨本規則通過後作必要調整，以使其適用同於本規則。

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(18) 本規則並未適用於當事人於其單純的個人或家庭活動中所為，並因此不涉及職業行為或商務活動之個人資料處理。個人或家庭活動得包括通信交流及持有地址資料，或社交網絡及此等活動範圍內所進行之網路活動。然而，本規則適用於此等個人或家庭活動中為個人資料處理提供媒介之控管者或處理者。

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and

of the Council[7]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

(19) 主管機關為達預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的所為當事人受保護之個人資料處理，包括為維護及預防此等資料對公共安全及個人資料自由流通造成之威脅，乃係特定歐盟法律之主題。因此，本規則不適用於有關上開目的所為之個人資料處理。惟公務機關依本規則處理個人資料時，如其使用係為上開目的，則應受更為具體之歐盟法案之拘束，即歐洲議會及歐盟理事會所制定之歐盟第 2016/680 號指令[7]。對於歐盟第 2016/680 號指令所定之主管機關，會員國得委託其非必然為上開預防、調查、偵查及追訴刑事犯罪或執行刑罰，包括為維護及預防對公共安全造成威脅之目的之職務，而該等非基於上開目的所處理之個人資料，仍屬於歐盟法之範疇，亦有本規則之適用。

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation,

---

[7] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).
歐洲議會及歐盟理事會於 2016 年 4 月 27 日就主管機關為達預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的，對於個人資料處理之保護及自由流通，制定歐盟第 2016/680 號指令，取代理事會框架決定第 2008/977/JHA 號（詳該官方公報第 89 頁）。

Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

關於主管機關在本規則之目的範圍內所處理之個人資料，會員國應得維持或採用更具體之規範，使其與本規則規定之適用相符。各會員國得自行斟酌其憲法、組織及行政法架構，為該等機關因上開目的以外所為個人資料之處理，訂定更具體化之特定規範。如私人處理個人資料在本規則之目的範圍內者，本規則應使會員國得於特定情況下以法律限制其權利義務，且該限制屬在民主社會中所必要且適度之措施，並係為維護特定重要利益，包括公共安全及預防、調查、偵查或追訴刑事犯罪或執行刑罰，包括維護及預防對公共安全之威脅。舉例而言，此關係到洗錢防制架構或鑑識實驗活動等。

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in

relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(20) 本規則之適用範圍雖包括但不限於法院及其他司法機關之活動，但歐盟法或會員國法仍得具體化規範該等法院及其他司法機關於處理個人資料時所應遵守之要點及程序。法院基於行使其司法權限所為個人資料之處理，為確保法院履行其司法任務時得以獨立審判，包括作成判決，監管機關不應干涉之。於會員國特別確保本規則所定規範之遵守，強化司法人員認知其於本規則下所負之義務，並受理關於處理此類個人資料所生之申訴時，該會員國得於其司法系統下設立監控此類個人資料處理之單位。

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council[8], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

---

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).
歐洲議會及歐盟理事會於 2000 年 6 月 8 日通過歐洲市場資訊社會服務，尤其是電子商務之特定法律觀點指令第 2000/31/EC 號（「電子商務指令」）（官方公報 L 類 178 期，2000 年 7 月 17 日，第 1 頁）。

(21) 本規則不影響歐洲議會及歐盟理事會[8]所定歐盟指令第 2000/31/EC 號之適用，特別是中介服務商依該指令第 12 至 15 條規定所負之義務。該指令旨在確保會員國間資訊社會服務之自由流通，以促進歐洲市場之正常運作。

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

(22) 控管者或處理者在歐盟境內之分支機構所為之一切個人資料處理均應受本規則之拘束，無論其處理行為本身是否發生於歐盟境內。分支機構係指透過穩定安排，從事於有效且實際之活動。此等安排之法律形式，不因其係透過分公司或具有法人格之子公司所為而有不同。

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details,

or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(23) 為確保當事人受本規則所保護之權利不被侵奪，凡為歐盟境內之資料主體，雖由非設立於歐盟境內之控管者及處理者進行個人資料處理，惟其處理活動涉及為該等資料主體提供商品或服務者，不問是否涉及付款，本規則仍應予適用。為決定控管者或處理者是否為歐盟境內之資料主體提供商品或服務，應確認是否明顯可知該控管者或處理者預見其係提供服務予位於一個或多個歐盟會員國境內之資料主體。如僅係可接近使用控管者、處理者或中介者於歐盟境內之網頁、電子郵件或其他聯繫方式，或所使用之語言係控管者設立地之第三國所通常使用之語言，均不足以確認其具有提供商品或服務之上述意圖；但諸如：所使用之語言或貨幣通常係使用於一個或多個會員國境內且有以該語言訂購其商品或服務之可能性，或所提及之消費者或使用者位於歐盟境內者，則可能使其明顯可知控管者擬向於歐盟境內之資料主體提供商品或服務。

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person,

particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(24) 凡為歐盟境內之資料主體，雖由非設立於歐盟境內之控管者及處理者進行個人資料處理，惟其涉及對該資料主體之行為所為監控且該受監控之行為係發生於歐盟境內者，本規則亦應予適用。為決定該資料處理是否可受認定為監控該資料主體之行為，應確認當事人是否於網路中被追蹤，包括以個人資料處理技術為潛在之後續使用而將當事人建檔，特別是為了得到其決策，或為分析或預測其個人喜好、行為及態度。

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(25) 凡會員國法律依國際公法可得適用之領域，本規則亦應拘束非設立於歐盟境內之控管者，諸如會員國之使領館。

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should

therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(26) 個人資料保護原則應適用於有關識別或可得識別當事人之任何資訊。已假名化之個人資料，且可透過使用額外資訊而識別出當事人身分者，應被認為屬於可得識別之當事人的資訊。為決定當事人是否可被識別，應考慮到所有可合理使用之方法，例如由控管者自己或透過他人指認以直接或間接地識別該當事人。為確認何為可合理使用作為識別當事人之方法，應考慮所有客觀因素，諸如：識別所需之成本與時間，並考慮到資料處理當時現有之技術及科技發展。因此，資料保護原則不適用於匿名資訊，亦即並非已識別或可識別當事人之資訊，或以使資料主體不可或不再可識別之方式而成為匿名之個人資料。因此，本規則無涉於此類匿名資訊之處理，包括為統計或研究目的所為之者。

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(27) 本規則不適用於死者之個人資料。會員國得自行規範關於死者之個人資料處理。

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(28) 對於個人資料採用假名技術可對資料主體降低風險，並可協助

控管者及處理者履行其保護個人資料之義務。本規則明確引用「假名化」並無意排除為資料保護目的所為之其他任何措施。

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(29) 為鼓勵於個人資料處理過程中應用假名化技術，當同一控管者，縱令允許一般分析，於已採取必要之技術及組織措施以確保處理過程中本規則被遵守且得識別特定資料主體之額外資訊已被分開存放者，假名化技術應仍有其應用可能。控管者於處理個人資料時應註明在同一控管者之被授權人。

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(30) 透過設備、應用程式、工具及通訊協定，諸如網際網路協定位址、瀏覽歷程記錄識別碼或其他識別工具，諸如無線射頻識別系統標籤，當事人可被連結到網路上識別碼。此可能留下軌跡，並可被用於對當事人建檔並識別其身分，特別是當該軌跡結合了唯一的識別碼及從服務商取得其他資料。

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission,

such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(31) 為執行公務而取得依法定義務所揭露個人資料之公務機關，諸如稅務機關及海關、金融調查單位、獨立行政機關或負責規範及監管證券市場之金融市場主管機關，如其接收個人資料係為公眾利益所必要而進行特定詢問者，該公務機關非屬歐盟法或會員國法所定之資料接收者。公務機關要求揭露應以書面、附理由且偶然為之，且不得通用於整個檔案系統或與其他檔案系統相聯通。公務機關處理個人資料應依照其處理之目的，遵守可適用之資料保護規則。

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent

should cover all processing activities carried out for the same purpose or purposes.When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(32) 同意之給予必須是資料主體依其意思決定就其個人資料處理所為具體肯定且自由形成、明確、受充分告知及非模糊之指示，諸如：口頭或書面之聲明，包括以電子方式為之者。同意可能包括於瀏覽網頁時所點選之選項、為資訊社會服務所做技術設定之選擇或其他聲明，或依其脈絡清楚顯示資料主體接受被提案之個人資料處理的行為。因此，單純沉默、預設選項為同意或不為表示不構成同意。同意應涵蓋基於相同之一個或多個目的所為之全部處理活動。如個人資料之處理具有多重目的者，應為全部目的取得同意。如資料主體之同意係基於電子方式之請求者，該請求必須清楚、簡潔且對所提供服務之使用不構成非必要之破壞。

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(33) 為科學研究目的所為之個人資料處理，於資料蒐集當時，通常不可能完整指明該處理之目的。因此，當科學研究符合公認之道德標準時，應允許資料主體僅就科學研究之特定範圍為同意之表示。資料主體應有機會僅就特定研究範圍或預期目的所允

許範圍內之部分研究計畫表示同意。

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(34) 基因資料係指經由當事人生物樣本分析後所涉及該當事人遺傳性或突變性之基因特徵之個人資料，特別是染色體、去氧核糖核酸（DNA）或核糖核酸（RNA）分析或從其他元素可獲得相同資料之分析。

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council[9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
歐洲議會及歐盟理事會於 2011 年 3 月 9 日就跨境醫療保健之病患權利制定歐盟指令第 2011/24/EU 號（官方公報 L 類第 88 期，2011 年 4 月 4 日，第 45 頁）。

(35) 關於健康之個人資料應包括資料主體所揭露關於過去、現在或未來生理或心理健康狀態而與該資料主體健康情況有關之全部資料。其中包括在為當事人登記之過程中或為其提供依照歐洲議會及歐盟理事會[10]所定第 2011/24/EU 號指令定義之醫療照顧服務中所蒐集之資訊；為醫療目的特別配予當事人而用以識別該人之號碼、標誌或獨特標識；對身體部位或組成物質（包括基因資料或生物樣本）進行測試或檢驗所得到之資訊；及從醫生或其他醫療專業人員、醫院、醫療裝置或體外診斷測試等獨立於資料主體以外來源所得之任何資訊，例如：疾病、殘疾、患病風險、病史、臨床治療或該資料主體之生理狀態或醫學狀態。

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor,

the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(36) 控管者於歐盟境內之主要分支機構應為其於歐盟境內核心管理機構之所在地，但個人資料處理的目的及方式係由控管者於歐盟境內另一分支機構所決定者，該分支機構應被視為主要分支機構。控管者於歐盟境內之主要分支機構應按客觀標準判定之，且其應經由穩定之安排而就個人資料處理之目的及方式等主要決策採取有效及有實際執行之管理行動。判定主要分支機構之標準不得取決於個人資料處理是否於該處所為之。為處理個人資料或其處理活動之技術方法或科技之存在與利用，其本身不構成主要分支機構，且因此並非主要分支機構之決定性標準。資料處理者之主要分支機構應為其於歐盟境內核心管理機構之所在地，或其於歐盟境內並無核心管理機構時，為其於歐盟境內為主要處理活動之所在地。於同時涉及控管者及處理者時，主管之領導監管機關應為控管者主要分支機構所在地會員國之監管機關，但處理者之監管機關應被視為係相關監管機關而應參與本規則所定之合作程序。在任何情況下，於裁決草案僅涉

及控管者時，有一個或多個分支機構之資料處理者所在之一個或多個會員國監管機關均不得視為係相關監管機關。個人資料處理係由企業集團實施者，控制企業之主要分支機構應被認定為企業集團之主要分支機構，但個人資料處理之目的及方式係由其他企業所決定者，不在此限。

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(37) 企業集團應包括控制企業及從屬企業，在此之控制企業應係能夠藉由諸如股權、資金參與或治理規範或執行個人資料保護規定之權力等方式對他企業發揮決定性影響力之企業。企業監控其關係企業之個人資料處理者，應將其與該等關係企業視為一企業集團。

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(38) 鑑於兒童或未盡知悉其個人資料處理之風險、後果及相關保護

措施及其權利，兒童就其個人資料值得受特別保護。特別保護尤應適用於為行銷或建立人格或使用者檔案之目的之兒童個人資料使用，及當使用直接提供予兒童之服務時兒童個人資料之蒐集。於直接向兒童提供預防性或諮詢性服務時，無須得其監護人之同意。

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step

should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(39) 個人資料之任何處理應合法且公正。個人資料之蒐集、利用、商議或其他處理應向當事人公開，且應及於該個人資料所處理或將處理之程度。透明原則要求關於個人資料處理之任何資訊或聯繫應方便取得、易於理解且應以清楚簡易之語言為之。透明原則尤其關注於向資料主體公開控管者身分、其處理資料之目的及進一步資訊，用以確保對於相關當事人為公正及透明之個人資料處理，並確保其得確認及溝通其所被處理之個人資料之權利。當事人應獲告知有關個人資料處理之風險、規範、保護措施及權利，以及其如何就該等處理行使其權利。特別是，個人資料處理之特定目的應具明確性及合法性，且應於蒐集個人資料時告確定。個人資料應適當、相關及限於其所受處理目的之必要範圍內。尤須確保個人資料之儲存期間係在最小限度範圍內。個人資料之處理唯有當其處理目的無法經由其他方式合理實現者始得為之。為確保個人資料未遭留存至超過其所必要之期間，控管者應設定個人資料銷毀之期限或定期確認之。各種合理措施應被採用以更正或刪除不正確之個人資料。個人資料之處理應以確保其適當安全性及保密性之方式為之，包括防止對個人資料及其處理過程所使用設備之未經授權之接近或使用。

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal

obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(40) 為合法處理個人資料，個人資料之處理應基於相關資料主體之同意或源自於法律規定（不論其為本規則或本規則所提及之其他歐盟法或會員國法規定）之其他合法性基礎，此包括控管者為遵守其法定義務所必要者，或資料主體作為契約當事人為契約履行所必要者，或於契約簽署前依據資料主體之要求所為者。

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(41) 凡本規則所指法律依據或立法措施，不以經議會採取立法行為為必要，但不得侵害依會員國憲法秩序之要求。惟法律依據或立法措施應清楚明確且為受規範者可得預見者，並應遵守歐盟法院及歐洲人權法院所定之判例法。

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[10]

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(42) 個人資料處理係基於資料主體之同意者，控管者應舉證證明資料主體同意該處理活動。尤其是在為他事件所為書面聲明時，保護措施應確保資料主體知悉其所為同意之事實及其同意之範圍。根據歐盟理事會所定第 93/13/EEC 號指令 [10]，控管者事先擬定之同意聲明書，應以易懂且方便取得之格式為之，並採用清楚簡易之語言，且不得有不公平條款。為同意所為之告知，資料主體至少應知悉控管者之身分及其個人資料處理所要達成之目的。於資料主體並非出於真意或無從自由選擇或其無法拒絕或無法於不損及其權益之情況下撤銷同意者，該同意應認定為不具自主性。

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent

---

歐盟理事會於 1993 年 4 月 5 日就消費者契約之不公平條款制定歐盟理事會指令第 93/13/EEC 號（官方公報 L 類第 95 期，1993 年 4 月 21 日，第 29 頁）。

on the consent despite such consent not being necessary for such performance.

(43) 為確保同意係自主作成，於資料主體與控管者間有顯著失衡之特定情況下，尤其於該控管者為公務機關且於該特定情況之整體情境下不可能有自主同意時，個人資料處理之同意欠缺有效之合法性基礎。於個別情況下應屬適當，卻不允許就不同個人資料處理方式為分別同意，或同意就契約履行非屬必要，卻將契約之履行（包括服務之提供）依存於該同意時，同意仍應推定為不具自主性。

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(44 於個人資料處理為契約所必要或為簽訂契約而有必要時，其處理應合乎法令。

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage

period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(45) 個人資料處理係基於控管者為遵守其法定義務所為，或係基於公共利益為履行任務所必要，或係公務機關行使公權力所必要者，該處理應具備歐盟法或會員國法之依據。本規則不要求就每一個別之處理定有具體法律規定。就控管者為遵守其法定義務所為、因公共利益為履行任務所必要或公務機關行使公權力所必要之數個處理方式明定其所依據之法律，可謂充分。其亦應由歐盟法或會員國法決定處理之目的。此外，該法得具體化規定本規則關於個人資料處理之合法性規範的一般條款、建構控管者之決定性標準、個人資料處理所涉個人資料之類型、相關個人資料主體、得向其揭露個人資料之實體、限制之目的、儲存期間及用以確保處理合法性與公正性之其他措施。歐盟法或會員國法亦應決定，為公共利益執行任務或行使公權力之控管者是否為公務機關或其他受公法所規範之個人或法人，或於其為公共利益所為之者時，是否包括為了如公眾健康與社會保障及健康照顧服務之管理等健康目的者、或依私法者，如職業工會。

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be

manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(46) 為保護資料主體或他人生活中之重大利益所必要者，個人資料之處理亦應被認定為合法。基於他人重大利益所為之個人資料處理，原則上僅有當該處理明顯無法基於其他法律依據為之者始得為之。有些處理類型得同時符合公共利益及資料主體重大利益之兩項重要理由，舉例而言，當個人資料之處理係基於人道目的所必要者，包括監測傳染病及其蔓延或人道救援之情況，特別是天災人禍之情形。

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the

legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(47) 控管者（包括個人資料得向其揭露之控管者）或第三方之正當利益，得作為資料處理之合法依據，但應兼顧該等利益或資料主體之基本權及自由，且考慮到資料主體基於其與控管者間關係所生之合理預期。正當利益可存在於諸如資料主體與控管者間具有相關且適當之關係，例如資料主體係控管者之客戶或由控管者提供其服務等情。無論如何，正當利益是否存在須審慎評估，包括資料主體於其個人資料之蒐集過程中及其當下是否能合理預期到該目的之資料處理。於個人資料處理係在資料主體無法合理預見其資料將被進一步處理之情況下所為者，資料主體之利益及基本權得特別優先於資料控管者之利益。鑑於公務機關處理個人資料之合法依據係由立法者以法律規範之，該合法依據不得適用於公務機關執行職務所為之個人資料處理。基於防範詐欺之目的而有個人資料處理之絕對需要者，亦得構成相關資料控管者之正當利益。為直接行銷之目的所為個人資料處理，得被認定係基於正當利益所為之。

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking

located in a third country remain unaffected.

(48) 身為企業集團之一部或隸屬於中央機構之組織之控管者，基於內部管理之目的，就企業集團內部間之個人資料傳輸，包括客戶或員工個人資料之處理，得有正當利益。企業集團內部間移轉個人資料之一般原則，於移轉至設址於第三國之企業者，亦同。

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(49) 為確保網路與資訊安全而嚴格遵循必要性及合比例性之個人資料處理（亦即，具有指定機密級別之網路或資訊系統，以防止突發事件或違法或惡意行為危害已儲存或已傳輸之個人資料之可用性、真實性、完整性及機密性，及危害藉由該等網路或系統、公務機關、資安危機應變小組（CERTs）、資安事件處理小組（CSIRTs）、電子通訊網路及服務供應商及安全技術服務供應商所提供相關服務之安全性），構成相關資料控管者之正當利益。舉例言之，此可能包括防止非經授權之電子通訊網路之

存取及阻擋惡意程式碼之散播及阻止「阻斷服務」攻擊及電腦及電子通訊系統之損害。

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

(50) 個人資料處理之目的非基於原蒐集該個人資料之目的者，唯有當處理及蒐集個人資料之目的得相互兼容者，始得為之。於此

類案件中，不需要有獨立於允許蒐集個人資料以外之合法依據。如個人資料之處理係為符合公共利益執行職務或委託控管者行使公權力所必須者，歐盟法或會員國法得決定及具體規範何等任務及目的所為之進階處理得被認定為具備兼容性及合法性。基於公共利益為達成上開目的、科學或歷史研究目的或統計目的所為之進階處理，應被認為屬於有兼容性及合法性之處理。歐盟法或會員國法為個人資料處理所訂定之合法依據亦得作為資料為進階處理之合法依據。為了確保進階處理之目的與原先蒐集資料之目的相互兼容，控管者於該當於原資料處理之全部合法性要件後，應考慮到包括但不限於：該等目的與所欲進階處理目的間之任何連結性；所蒐集個人資料之背景，尤其是資料主體基於其與控管者間之關係而對於進階使用之合理預見性；個人資料之本身性質；所欲進階處理對於資料主體造成之後果；及原處理與所欲進階處理作業中是否存在適當保護措施。

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited

if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

凡經資料主體之同意或係歐盟法或會員國法所定於民主社會中用以確保特別如一般公眾利益之重要目的所必要且成比例之措施者，不問目的間之兼容性，進階處理個人資料應予允許。在任何情況下，本規則所定原則之適用及特別是關於其他目的所知之資料主體之資訊及其包括拒絕權等權利均應予確保。由控管者指出可能之犯罪行為或對於公共安全之威脅，以及將特定案件或相同犯罪行為之相關案件或造成公共安全威脅所涉及之相關個人資料傳輸予主管機關，應被認定係控管者所作為之正當利益。惟如進階處理未遵守法定、專業或其他有拘束力之保密義務者，控管者基於正當利益所為之傳輸或進階處理應予禁止。

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for

the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(51) 依其本質對基本權及自由特別敏感之個人資料，因其處理過程中可能對於基本權及自由造成顯著風險，故值得受到特別保護。該等個人資料應包括顯示出種族或人種之個人資料，但本規則使用「種族」乙詞並不代表歐盟承認旨於區別個別種族存在之理論。照片之處理不應被制式化地認為係特殊類型之個人資料處理，蓋僅有在透過特殊識別方法之處理而得獨特識別或驗證出當事人時，始得將照片涵蓋於生物特徵識別資料的定義之下。該等個人資料不得處理，但其處理係本規則明定之特別情況所允許，且考量到會員國法為使其與本規則規定之適用相符以遵守其法定義務或符合公共利益執行職務或委託控管者行使公權力而對於資料保護定有具體規範者，不在此限。除就該等處理所定之特別要件以外，本規則所定之一般原則及其他規定亦應予適用，尤其是涉及處理之合法性要件。為特殊類型之個人資料處理所設一般禁止規定之例外，應予明確規定，包括：資料主體明確同意或涉及特殊需求之資料處理，尤其是基於實現基本自由之目的而為某些組織或基金會之正當活動所為之處理者。

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or

Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(52) 於歐盟法或會員國法已有明文且有適當保護措施以保護個人資料及其他基本權之情況下，為基於公共利益之目的，特別是在勞動法、包括退休金及安全衛生等社會法領域、監控及警示目的、傳染病及其他對於健康造成重大威脅之疾病預防及控制所為之個人資料處理，特殊類型個人資料處理之禁止規定亦應允許例外。基於健康目的，包括公共衛生及醫療保健服務之管理，特別是為確保醫療保險制度中處理福利及服務訴求之程序的品質與效益，或是符合公共利益之存檔目的、科學或歷史研究或統計目的，該等例外規定得以為之。為建構、行使或防禦法律上之請求而有必要者，不問係於訴訟程序或行政程序或於法院以外之程序，該等個人資料處理之禁止規定亦應允許例外。

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and

society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(53) 值得受較高度保護之特殊類型個人資料，於下述情形始得處理之，亦即：僅有基於與健康相關之目的，且基於全體人類及社會整體之利益為達成該等目的所必要者，特別是在健康或社會照護服務及系統之管理，包括為品質控制、管理資訊及一般國內及地方監管健康或社會照護系統之目的管理及整合國內醫療院所之該等資料之處理，以及為確保健康或社會照護及跨境醫療保健或健康安全之永續性、為監控及警示目的或符合公共利

益之存檔目的、科學或歷史研究或統計目的、基於符合公共利益目的之歐盟法或會員國法以及符合公共利益在公共衛生領域所為之研究。因此，本規則應就涉及健康之該等特殊類型個人資料之處理，針對特殊需求，為一致性之規範，尤其是該等資料之處理係為特定醫療相關目的，由因職業持有秘密而負法定保密義務之人所為之者。歐盟法或會員國法應明文規定具體適當之措施，以保障個人基本權及其個人資料。會員國應被允許維持或採用進一步規定，包括但不限於關於基因資料、生物特徵識別資訊或與健康相關資訊之個人資料處理。惟該等條款適用於該等個人資料之跨境處理時，不得妨礙個人資料於歐盟境內之自由流通。

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council[11], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).
歐洲議會及歐盟理事會於 2008 年 12 月 16 日就公共衛生及工作安全衛生之區域統計訂定歐盟規則第 1338/2008 號（官方公報 L 類第 354 期，2008 年 12 月 31 日，第 70 頁）。

such as employers or insurance and banking companies.

(54) 未取得資料主體同意之特殊類型個人資料處理，於公共衛生領域基於公共利益之理由可能是有必要的。該等處理應受適當具體措施之拘束以維護當事人之權利及自由。就此，「公共衛生」應以歐洲議會及歐盟理事會[11]第 1338/2008 號歐盟規則所作定義而為解釋，亦即與健康有關之全部要素（即健康狀況），包括疾病與殘疾、對於健康狀態產生影響之決定性因素、醫療保健之需求、醫療保健之資源分配、醫療保健之提供及普及性以及醫療保健之開支及財務規劃及致死率之起因。以公共利益為由所為涉及健康資料之該等處理，不得因其他目的而由諸如雇主或保險公司及銀行等第三人為處理。

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(55) 再者，機關所為個人資料處理係為實現官方所認可之宗教組織所定符合憲法或國際公法之目標者，應屬具備公共利益之基礎。

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(56) 凡於選舉活動過程中，會員國內民主制度之運作要求政黨編纂關於人民政治觀點之個人資料，於建構適當保護措施之情況下，基於公共利益之理由，該等資料處理得予准許。

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision

of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(57) 於經資料控管者處理之個人資料不允許其識別該當事人時，資料控管者即不得單獨為達成本規則之任何條款之目的，為識別資料主體而獲取額外資訊。但控管者不得拒絕接受資料主體為行使其權利所提供之額外資訊。識別應包括資料主體之數位辨識在內，例如透過資料主體登入資料控管者提供之網路服務時所使用之相同憑證等認證機制。

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(58) 透明原則要求任何傳達予公眾或資料主體之資訊皆須簡潔、容易取得且容易理解，以清楚簡易之語言作成，並且適當地視覺化。該等資訊之提供得以電子形式，例如要傳達給公眾時透過

網站呈現。尤其於行為者繁多且實務技術複雜之情形，會造成資料主體難以知悉並理解其個人資料是否、由誰、以什麼目的被蒐集，例如網路廣告之情形。有鑑於兒童值得特別保護，任何提供予兒童之資訊及溝通應採用兒童易於理解之清楚簡易之語言。

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(59) 為利於資料主體行使本規則之權利，應提供不同之免費管道，包括請求之機制及（如有可能）獲得之機制，尤其是接近並更正或刪除個人資料及行使拒絕權。控管者亦應提供電子化請求之方式，特別是於個人資料係以電子方式處理時。控管者有義務回應資料主體之請求，不得無故遲延且最遲於一個月內為之，並於控管者不同意該等請求時附具理由。

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed

whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(60) 公平及透明處理原則要求資料主體須受處理方式及其目的之通知。控管者應提供資料主體任何需要之進一步資訊以確保考慮到個人資料處理之特定情形及過程而為公平及透明之處理。再者，資料之建檔及其建檔結果應通知資料主體。當個人資料係收集自資料主體時，資料主體應獲告知其是否有義務提供個人資料及不提供該等資料時之結果。該資訊得以標準化之標誌方式提供，俾提供易見、易懂且清晰易讀之方式，並對於所欲為之處理進行有意義之概述。於標誌係以電子方式表示時，其須得由機器辨認之。

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(61) 與資料主體之個人資料處理有關之資訊，應於向資料主體蒐集資料時，或從其他來源取得該個人資料時，在依個案判定之合理時間內，給予資料主體。於個人資料得合法揭露予其他接收者時，亦應於揭露予接收者之初即通知資料主體。控管者欲基於原蒐集目的外之目的處理個人資料時，控管者應事先將進階處理之其他目的之資訊及其他必要資訊提供資料主體。當個人資料之來源因來源眾多以致無法提供給資料主體時，應提供概括之資訊。

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(62) 然而，於資料主體已持有資訊，個人資料之儲存或揭露業經法律規定，或經證明不可能提供資訊予資料主體，或提供資訊須花費過鉅之勞費時，資訊提供義務之課予即無必要。後者情形尤其發生於處理資訊係為了公共利益、科學或歷史研究目的或統計目的。此際，資料主體之數量、資料之年代以及其他適當之保護措施皆應考慮在內。

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as

diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(63) 資料主體應有權接近使用其所受蒐集之個人資料，並得容易地、於合理之時間間隔行使接近使用權，以知悉並核實該處理之合法性。此包括資料主體有權接近使用其健康資訊，例如包括診斷、檢驗結果、醫師所為評鑑及任何治療或干擾措施提供之資訊。因此，各資料主體應有權知悉及獲得溝通，尤其是個人資料受處理之目的、受處理之可能期間、個人資料之接收者、任何自動處理個人資料所涉及之邏輯、以及至少於建檔時之資料處理結果。若有可能，控管者應提供得遠端使用之安全系統以提供資料主體對其個人資料有直接之接近使用權。該權利不得對他人之權利或自由有不利之影響，包括營業秘密或智慧財產權，尤其是保護軟體之著作權。但是，就此等面向之顧慮不得

導致拒絕提供所有資訊予資料主體之結果。當控管者處理有關資料主體之大量資訊時，應得於資訊傳遞前請求資料主體特定與其請求相關之資訊或處理活動。

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(64) 控管者應使用所有合理手段以驗證請求接近使用資料之資料主體的身分，尤其是在網路服務或網路識別工具之情形。控管者不得為了回應潛在請求之單獨目的而獲取個人資訊。

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,

on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(65) 資料主體應有更正其個人資料之權利、以及當資料保存違反規範控管者之本規則、歐盟法或會員國法時應有「被遺忘權」。尤其，資料主體應享有刪除其個人資料之權利，並於該個人資料就資料蒐集或另為處理之目的已無必要時、於資料主體已撤回其同意或拒絕其個人資料之處理時、或於其個人資料處理違反本規則時，資料主體應享有請求不再處理其個人資料之權利。該權利尤其涉及該資料主體於兒童時期所為同意且未完整理解該處理存在之風險，爾後希望移除其個人資料（特別是網路上資料）之情形。不問其是否仍為兒童，資料主體應得行使該權利。然而，為了表意自由權之行使、法律義務之遵守、符合公共利益之職務執行、或委託控管者行使公權力所必須者、在公共衛生領域上之公共利益的理由、為了實現公共利益、科學或歷史研究目的或統計目的時、或為了建立、行使或防禦法律上主張時，於必要範圍內進一步保留個人資料應屬合法。

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(66) 為強化網路環境之被遺忘權，刪除權亦應擴張至公開個人資訊之控管者有義務通知個人資料處理之控管者刪去任何該個人資

料之連結、複製或仿製。透過此種做法，該控管者應採取合理步驟，考量現有科技與對控管者可行之手段，包括科技方式，通知依該資料主體之請求而正在處理該個人資料之控管者。

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(67) 限制個人資料處理之方法得包括但不限於暫時將選取之資料移至其他處理系統、使選取之個人資料無法被使用者取得，或暫時移除網站上已公開之資料。於自動歸檔系統中，處理之限制原則上應以科技方式確保個人資料不會繼續成為進一步處理活動之對象且不能改變。系統中應明確指出個人資料之處理受到限制之事實。

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against

controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(68) 為了進一步強化對自己資料之掌控，當個人資料以自動化手段執行處理時，資料主體亦應有權以有結構的、通常使用的、機器可讀的，且可共同操作的形式接收其提供予控管者之資料，並有權將之傳輸給其他控管者。資料控管者應被鼓勵發展使資料具可攜性之可共同操作模式。於資料主體基於其同意提供個人資料或資料處理係履行契約所必要者，該權利應有其適用。當資料處理係基於法律理由而非本於同意或契約時，則應無其適用。基於其此項本質，該權利不應於控管者為執行公共任務而處理個人資料時有其適用。因此，當個人資料之處理係基於

控管者遵守其法律義務、或符合公共利益之執行職務、或委託控管者行使公權力所必須者，該權利即不予適用。資料主體傳輸或接收其個人資料之權利不應導致控管者有義務採取或維持技術上得兼容之處理系統。在不僅涉及單一資料主體之一系列個人資料中，接收個人資料之權利不應損及其他資料主體依本規則所享有之權利與自由。再者，該權利不應損及資料主體得刪除其個人資料之權利，以及該權利在本規則中所受到的限制，尤其不應推認資料主體在履行契約之範圍內提供其為履行契約所必要之個人資料得予刪除。當技術上可行時，資料主體應有權直接從一控管者傳輸其個人資料至另一控管者。

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(69) 然而，於個人資料得被合法處理係因有處理之必要且符合公共利益之執行職務、或委託控管者行使公權力、或基於控管者或第三人之有正當利益之理由時，資料主體仍應有權基於其特殊情形拒絕任何個人資料之處理。此時應由控管者證明其正當利益優先於資料主體之利益或基本權與自由。

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly

brought to the attention of the data subject and presented clearly and separately from any other information.

(70) 當個人資料之處理係以直接行銷為目的時，資料主體應有權在任何時間且毋需任何費用拒絕該處理，包括在與直接行銷有關之範圍內建檔，而不問係原始處理或進階處理。應明確提請資料主體注意該權利，且清楚表達並與其他訊息區別。

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain

human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

(71) 資料主體應有權不受決策之拘束，該決策可能包括對其產生法律效果或類似之重大影響並僅以自動化處理來評估其個人特徵之措施，例如網路貸款申請之自動拒絕或不包括任何人為介入之電子化招募。該處理包括評估個人特徵之個人資料自動化處理的任何形式之「建檔」，尤其是為了分析或預測有關資料主體之工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、地點或動向等特徵，而會對其產生法律效果或類似之重大影響者。然而，在控管者受拘束之歐盟法或會員國法有明文授權時，基於該處理所作成之決策（包括建檔）應予允許，此包括為監控及預防詐騙及逃漏稅之目的，依歐盟機構或國家層級監督機構之規範、標準及建議所為之者，以及為確保控管者提供服務之安全性與可信度，或為締結或履行資料主體與控管者間之契約所必要者，或於資料主體曾給予明確同意之情形。在任何情況下，該處理應有適當之保護措施，此應包括將特定資訊給予資料主體及獲得人為干預、表達意見、獲得依上開評估後做成決策之解釋，以及挑戰該決策之權利。該措施不得涉及兒童。

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data

subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.
為了確保對於資料主體之公平與透明的資料處理，於考慮個人資料處理之特定情況與脈絡時，控管者應於建檔時使用適當之計算或統計程序、應實施科技化且有組織的措施以適度確保尤其是可使個人資料不準確性得以更正及將錯誤風險最小化的要素，並應在考慮資料主體的利益與權利所受潛在風險，及預防包括但不限於基於種族或人種、政治意見、宗教或信仰、貿易聯盟會員、基因或健康狀態或性傾向等理由對當事人之歧視效果或造成此種效果之態度下，保護個人資料。基於特殊類型之個人資料所為之自動決策與建檔只有在特定條件下始被允許。

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(72) 建檔受本規則規範個人資料處理之規定所拘束，例如關於處理或資料保護原則之法律基礎。本規則所創立之歐洲資料保護委員會（「委員會」）應在此脈絡下提出指導。

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security,

including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(73) 關於特定原則與資訊權、接近使用權、更正或刪除個人資料之權利、資料可攜性之權利、拒絕權、基於建檔之決策、以及對資料主體之個人資料受侵害時之溝通與控管者之特定義務，於下述範圍內，歐盟法或會員國法得施加限制，亦即：在民主社會中所必要且適度用以維護公眾安全者，包括保護人民生命，特別是自然或人為災害之應變、預防、調查及追訴刑事犯罪或執行刑罰，包括為維護及預防對公共安全造成之威脅、或違反特定職業之道德規範、歐盟或會員國之一般公共利益的其他重要宗旨，尤其是歐盟或會員國之重要經濟或金融利益、為一般公共利益為由所留存之公共紀錄之保存、進階處理已歸檔之個人資料以提供有關前極權主義國家機制下之政治行為之特定資訊、或保護資料主體或其他人之權利及自由，包括社會保護、公共衛生與人道目的。此等限制應合乎憲章及歐洲保護人權與

基本自由公約所定之要求。

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(74) 有關控管者或其代表所為任何個人資料處理之控管者責任與義務應予確立。尤其，控管者有義務執行適當且有效之措施，並可證明其處理活動符合本規則，包括該措施之有效性。該措施應考量資料處理之本質、範圍、過程與目的，以及對當事人權利與自由之風險。

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health,

personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(75) 當事人之權利及自由所受之諸多可能且嚴重之風險，可能起因自處理個人資料，並造成身體上、物質上、或非物質上之損害，尤其是於下述情形時：當處理可能造成歧視、身分盜用或詐欺、金融損失、名譽損害、受職業性秘密保護之個人資料之機密性喪失、假名化未授權撤銷、或其他任何顯著之經濟性或社會性之不利益時；當資料主體之權利或自由可能受到剝奪或被排除在自己之個人資料控制權之外時；當個人資料處理涉及揭露種族或人種、政治意見、宗教或哲學信仰、貿易聯盟會員、以及基因資料之處理、有關健康之資料或有關性生活或前科及犯罪或相關保安措施之資料時；當個人特徵受到評估，尤其是為了建檔或使用個人檔案，分析或預測有關工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、地點或動向等個人特徵時；當處理易受傷害之個人（尤其是兒童）之個人資料時；或當該處理會牽涉大量個人資料並影響大量資料主體時。

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(76) 資料主體之權利與自由所受風險之嚴重性及可能性應參考資料處理之本質、範圍、過程與目的定之。風險應在客觀評鑑基礎上被評估，並藉以確定資料處理活動是否有風險或有高度風險。

(77) Guidance on the implementation of appropriate measures and on

the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(77) 有關執行適當措施與有關控管者或處理者所應遵守規範之指導原則（尤其是有關資料處理所涉及之風險的識別，對於其來源、本質、可能性與嚴重性、以及降低風險之最佳方法），得被以特別是下列方式提供，亦即得以經核准之行為守則、經核准之認證、委員會提供指導原則或資料保護員之指示等方式提供。委員會亦得頒布較不可能導致對於權利或自由有高風險之處理活動的指導原則，並指出何種措施足以解決此等風險。

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using

applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(78) 關於個人資料處理之權利及自由保護必須採取適當之科技化且有組織的措施，以確保符合本規則之要求。為了得以證明符合本規則，控管者應採取符合特別是設計與預設資料保護原則之內部規則與執行措施。該等措施得包括但不限於個人資料處理之最小化、盡可能將個人資料予以假名化、個人資料之處理與作用予以透明化、使資料主體得以監控該資料處理、使控管者得以創造與提升安全功能。在開發、設計及選用處理個人資料或透過處理個人資料完成其任務之應用程式、服務與產品時，產品、服務與應用程式之製造者應被鼓勵在開發與設計此類產品、應用程式時將資料保護權納入考量，並在考慮適當之技術狀態下，確保控管者和處理者得以完成其資料保護之義務。在公開招標之過程中，設計與預設資料保護原則亦應納入考量。

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(79) 資料主體之權利與自由保護與控管者及處理者之責任與義務（此也均與監管機關之監控與其手段有關）應依本規則予以明確分

配，包括於控管者與其他控管者共同決定資料處理之目的與手段時，或是由控管者之代表進行處理活動時。

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(80) 非設立於歐盟之控管者或處理者處理歐盟內資料主體之個人資料，且其處理活動涉及提供貨品或服務時，不問是否需要資料主體付款，對該等資料主體或對就其發生於歐盟內行為之監控，

控管者或處理者皆應指定其代表，但該處理係出於偶然、不含括大規模涉及特殊類型之個人資料處理、或涉及前科及犯罪之個人資料的處理，且考量處理之本質、過程、範圍與目的，其不會對當事人之權利與自由造成風險、或控管者是公務機關或機構者，不在此限。該代表應代表控管者或處理者，且得受任何監管機關之監管。控管者或處理者應明確以書面委託該代表履行其依照本規則所負之義務。該指定不影響控管者或處理者基於本規則之責任或義務。該代表應依據控管者或處理者之委託執行其任務，包括為確保符合本規則而須與主管機關合作之任何作為。於控管者或處理者不守法時，受指定之代表應為執行程序之對象。

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor

may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(81) 為確保處理者代控管者執行處理活動時遵循本規則，當委託處理者處理活動時，控管者應只委託具有足夠保證（尤其是就專業知識、可信度與資源而言）之處理者，以符合本規則之要求而執行科技化與組織化之措施，包括處理之安全性。處理者採取經核准的行為守則或認證機制可用以證明其有遵循控管者之義務。處理者就處理之執行應受到契約或符合歐盟法或會員國法之其他法規控管，將處理者結合至控管者、明列主體事項及處理持續之時間、處理之本質與目的、個人資料之類型及資料主體之分類，並考慮所欲執行之處理脈絡下處理者之特定任務與責任，以及資料主體之權利與自由的風險。控管者與處理者得選擇使用個別性契約或定型化契約條款，該條款須或為執委會所直接採用，或經監管機關以一致性機制再由執委會所採用者。代表控管者完成處理後，基於控管者之選擇，處理者應返還或刪除個人資料，除非處理者所受拘束之歐盟法或會員國法要求處理者儲存個人資料。

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(82) 為證明遵循本規則，控管者或處理者應依其職責保留處理活動之紀錄。各控管者及處理者應有義務配合監管機關並做成前開紀錄，並依要求提供之，使處理活動受監控。

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(83) 為維持安全性與預防資料處理違反本規則，控管者或處理者應評估與處理相關之風險，並執行相關措施以降低風險，例如加密。該等措施應確保適當之安全程度，包括機密性，且考慮到有關欲保護之個人資料的風險及本質之現有技術狀況與執行費用。於衡量資料安全風險時，應考慮因個人資料處理所造成之風險，例如意外或非法破壞、遺失、變更、未獲授權之揭露或接近使用、個人資料之傳輸、儲存或其他可能特別引起身體上、物質上或非物質上之損害。

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account

when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(84) 就處理活動可能造成當事人之權利或自由有高度風險之情形，為了促進對本規則之遵守，控管者應負責執行資料保護影響評估，以衡量（特別是）風險的來源、本質、特殊性與嚴重性。為證明個人資料之處理符合本規則，在決定適當措施時，評估結果應納入考量。當資料保護影響評估指出處理活動涉及高度風險而控管者無法以現有技術及執行成本提供適當措施降低風險時，應於處理前徵詢監管機關。

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be

provided in phases without undue further delay.

(85) 若未受到適當且及時之處理，個人資料之侵害可能造成當事人之身體上、物質上或非物質上損害，例如喪失對其個人資料之控制或對其權利之限制、歧視、身分盜用或詐欺、金融損失、假名化未授權撤銷、名譽損害、受職業性秘密保護之個人資料之機密性喪失、或其他任何對於所涉當事人之顯著經濟性或社會性之不利益。因此，一旦控管者發現個人資料侵害已然發生，即應向監管機關通報，不得無故遲延，且若可能，應於發現後 72 小時內通報，但控管者得證明依照歸責原則該個人資料之侵害不可能造成當事人之權利與自由的風險者，不在此限。當該通知無法於 72 小時內到達時，遲延之原因應與通知一併提供，且不得有更進一步無故遲延。

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(86) 當個人資料侵害可能造成當事人之權利或自由之高度風險，為了使其得以採取必要之防範措施，控管者應與資料主體溝通個人資料之侵害，不得無故遲延。該溝通應描述個人資料侵害之

本質及對該當事人降低潛在不利影響之建議。此種對資料主體之溝通應儘快、合理、可行，且與監管機關密切合作，遵守監管機關或其他相關機關如執法機關之指導。例如，降低損害之立即風險的需求即需要立刻與資料主體溝通，但執行適當措施以對抗繼續或類似的個人資料侵害之需求則得正當化較長之溝通時間。

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(87) 應查明是否已實行所有適當之技術保護與組織措施以立即確定個人資料侵害是否發生並快速通知監管機關與資料主體。該通知非無故遲延之事實尤需考量對個人資料侵害之本質與嚴重性及其對資料主體之結果與不利影響。該通知可能導致監管機關依據本規則所定任務與權力之介入。

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a

personal data breach.

(88) 在訂定個人資料侵害之通知所適用關於形式上及程序上之細節性規定時，應適當考量侵害之情形，包括個人資料是否已受到適當技術保護措施之保護、有效限制身分詐騙或其他形式濫用之可能性。此外，當及早揭露可能會無謂妨礙對於個人資料侵害情形之調查者，該等規定與程序應考量執法機關之正當利益。

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(89) 歐盟指令第 95/46/EC 號規範了向監管機關通知個人資料處理之一般性義務。然而該義務造成了行政與財政上之負擔，並非所有情形都對提升個人資料之保護有所助益。因此，該未加區別之普遍通知義務應予廢除，並改以注重依處理活動之本質、範圍、脈絡及目的等特徵區分容易對當事人權利與自由造成高風險之種類的更有效程序與機制加以取代。該處理活動之種類尤其可能是涉及新技術之使用，或未曾由控管者實施資料保護影響評估或基於自開始處理所經過之時間而有必要之新類型處理活動。

(90) In such cases, a data protection impact assessment should be carried

out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(90) 在此種情形，控管者應在處理之前進行資料保護影響評估，以評估高風險之特定可能性與嚴重性，並考量處理之本質、範圍、脈絡與目的及風險來源。該影響評估尤其應包括預計用以降低風險、確保個人資料保護與顯示遵循本規則之措施、保護措施與機制。

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations

where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(91) 此尤其適用於預定處理地區、國家或超國家層級可觀數量之個人資料，且可能影響大量資料主體並導致高風險之大規模處理活動，例如，基於其敏感性，按照現存技術知識狀況，大規模使用新技術並用於對資料主體之權利與自由造成高風險之其他處理活動，尤其是該等活動使得資料主體更難以行使其權利者。透過建檔資料，就相關當事人之個人特徵為體系性及密集性之評估、或透過特殊類型之個人資料、生物資料、或前科及犯罪資料或相關保安措施等之資料處理，以取得特定當事人之決策所為之個人資料處理者，亦應進行資料保護影響評估。資料保護影響評估也在大規模監控公共場合時有其必要，特別是使用光學電子裝置或主管監管機關認為該處理有可能對資料主體之權利與自由造成高風險之任何其他活動，尤其是因該等裝置或活動使資料主體無法行使權利、或使用服務或契約，或是因其係被有系統性地大規模執行者。若由個別醫生、其他健康照護專業者或律師處理來自於病患或客戶之個人資料時，不應被視為大規模之處理。在此種情形，資料保護影響評估並非強制。

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing

platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(92) 有些情況下，資料保護影響評估之主體比單一計畫更廣泛將是合理且經濟的，例如，當公務機關或機構欲建立普遍性的應用程式或處理平台、或當許多控管者計畫引進普遍性的應用程式或跨產業或跨界之處理環境，或為廣泛使用的水平整合活動。

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(93) 於公務機關或公務機構執行任務係依據會員國法，且其所通過之內容係在規範相關之特定或系列處理活動時，，該會員國得視其為有必要在處理活動前進行該等評估。

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing

operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(94) 當資料保護影響評估指出某處理在缺乏保護措施、安全措施及機制以降低風險時可能導致對當事人之權利與自由有高風險，且控管者同意該風險無法在可及技術及執行成本下以合理措施降低時，應於處理活動開始前向監管機關諮詢。此種高風險可能肇因於某類型之處理及處理之程度與頻率，也可能導致損害之實現與對當事人之權利與自由之干擾。監管機關應於特定期限內回應諮詢之請求。然而，監管機關於一定期限內之不作為不應損及監管機關依照本規則所定之任務與權力所為之任何介入。作為諮詢過程之一部分，為待決資料處理所執行之資料保護影響評估結果得提交予監管機關，尤其是預定用以降低對當事人權利與自由之風險的措施。

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(95) 當有必要且受到請求時，處理者應協助控管者確實遵循衍生自執行資料保護影響評估之義務及衍生自先前監管機關諮詢之義務。

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(96) 規範個人資料處理之立法或行政措施之準備階段亦應進行監管

機關之諮詢，以確保所欲進行之處理遵循本規則，尤其要降低資料主體所涉之風險。

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(97) 於下述情形時，就資料保護之法律與實務有專業知識者應協助控管者或處理者內部監督本規則之遵守，亦即：當資料處理係由除了法院和獨立司法機關執行其司法權之公務機關執行時、於私部門之處理係由核心活動包括需要經常且有體系的監控大規模資料主體的控管者所為之處理活動、或於控管者及處理者之核心活動包括處理大規模特殊類型之個人資料及涉及前科及犯罪之資料時。在私部門中，控管者之核心活動係連結到其主要活動，而與作為輔助活動之個人資料處理無關。專業知識所需程度尤應依據所執行之資料處理活動及由控管者或處理者處

理之個人資料所需之保護而定。該等資料保護員，不問是否為控管者之雇員，都應以獨立之態度堅守職位以執行其任務。

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(98) 應鼓勵組織與代表控管者或處理者類型之其他機構在合乎本規則之限制下訂立行為守則，以促進本規則之有效適用，並考量某些行業執行資料處理之特定特徵及微型、中小型企業之特定需求。尤其，此種行為守則可能標誌出控管者與處理者之義務，考量資料處理可能造成當事人之權利與自由的風險。

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(99) 訂立行為守則或修改、擴張該守則時，組織與其他代表控管者或處理者類型之其他機構應諮詢利害關係人，包括如可行時之資料主體，並關注為回應此種諮詢所收到之意見及表達之觀點。

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(100) 為了提升本規則之透明度與對本規則之遵循，應鼓勵認證機制與資料保護標章及標誌之建立，使資料主體得快速評估相關產品及服務之資料保護程度。

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(101) 為了國際貿易與國際合作，進出非歐盟國及國際組織之個人資料流通是有必要的。該等流通之增加已然帶來了新挑戰與有關個人資料保護之問題。然而，當個人資料從歐盟移轉至第三國境內之控管者、處理者或其他接收者或國際組織時，在歐盟內依本規則對當事人保護之程度不得降低，此包括在從第三國或國際組織再移轉個人資料予在相同或其他第三國之控管者、處理者或再移轉至國際組織之情形。在任何情況下，向第三國和國際組織之移轉僅得於完全遵循本規則之前提下執行。唯有當控管者或處理者已遵守本規則所定關於個人資料移轉至第三國

或國際組織之規範，且受本規則所定其他條款之拘束者，個人資料之移轉始得為之。

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(102) 本規則不妨害歐盟與第三國間所締結用以規範包括對資料主體適當保障之個人資料移轉的國際協定。只要國際協定不影響本規則或歐盟法所定任何其他規範且包括對資料主體之基本權之適當程度的保障，會員國得締結涉及個人資料移轉至第三國或國際組織之國際協定。

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(103) 執委會得做成影響全歐盟之決定，認定第三國、第三國內之領域或特定部門，或國際組織已提供充足程度之資料保護，並因此就第三國或國際組織被認為已提供該保護程度乙事在整個歐

盟提供了法明確性和一致性。於該等情形，個人資料移轉至第三國或國際組織可能在不需要獲得進一步授權之情形下發生。於給予第三國或國際組織通知及說明理由之完全陳述時，執委會亦可決定撤銷原決定。

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(104) 依循歐盟所創立之基本價值，尤其是人權之保護，執委會在其衡量第三國或第三國內之領域或特定部門時，應考量特定第三國如何遵守法治、接近使用司法、以及國際人權規範和標準及其普通法與部門法，包括涉及公共安全、防禦與國家安全與公共秩序及刑法之立法。對第三國內之領域或特定部門作成有提

供充足保護之決定應考量明確與具體之標準，例如特定處理活動及第三國可適用之法律標準與立法之範圍。第三國應提供保證，以確保基本上等同於歐盟所保障之充足程度保護，特別是當個人資料處理在單一或數個特定部門時。尤其，第三國應確保有效而獨立之資料保護監督機制，且應提供合作機制予會員國資料保護機關，且應提供資料保護主體有效且可實現的權利與有效的行政與司法救濟。

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(105) 除了第三國或國際組織已加入之國際協約，執委會應考量第三國或國際組織於多邊或區域體系之義務，尤其是涉及個人資料保護及該等義務之履行。尤其，應考量第三國加入歐洲理事會 1981 年 1 月 28 日關於自動化個人資料處理之個人保護公約及其附加議定書。於衡量第三國或國際組織之保護程度時，執委會應向委員會諮詢。

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions,

the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council[12] as established under this Regulation, to the European Parliament and to the Council.

(106) 執委會應觀察審視第三國、第三國境內之領域或特定部門、或國際組織保護程度之決定的運作，並觀察審視在歐盟指令第 95/46/EC 號第 25 條第 6 項及第 26 條第 4 項之基礎下採行之決定。就有提供充足保護之決定，執委會應提供定期檢驗其運作之機制。該定期檢驗應在諮詢有關之第三國或國際組織下進行，且考量所有相關第三國或國際組織之發展。為了觀察審視與執行定期檢驗，執委會應考慮歐洲議會及歐盟理事會以及相關機構與來源之意見與認定。執委會應在合理時間內評估前次決定之運作情形，並如本規則所確立的，依歐洲議會及歐盟理事會之歐盟規則第 182/2011 號 [12]，向委員會報告任何相關認定。

(107) The Commission may recognise that a third country, a territory

---

[12] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
歐洲議會及歐盟理事會於 2011 年 2 月 16 日關於會員國之委員會行使執行權力之控制機制的規範與一般原則（官方公報 L 類第 55 期，2011 年 2 月 28 日，第 13 頁）。

or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(107) 執委會可能認定第三國、第三國內之領域或特定部門、或國際組織不再達到充足程度之資料保護。因此，向該第三國或國際組織之個人資料移轉應被禁止，但完成本規則關於移轉所定適當保護措施之要件被滿足，包括有拘束力之企業守則及存在特定情況之例外者，不在此限。在該情況，該規範應由執委會及該第三國或國際組織間訂定。執委會應於適當時間內通知第三國或國際組織其理由，並進入協商程序以救濟該情形。

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and

to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(108) 在欠缺有提供充足保護之決定時，控管者或處理者應為資料主體採取適當保護措施，以彌補第三國對資料保護之欠缺。該等適當保護措施可能包括利用有拘束力之企業守則、執委會採用之標準資料保護條款、監管機關採用之標準資料保護條款或由監管機關授權之契約條款。該等保護措施應確保符合資料保護之要求及資料主體之權利在歐盟境內適當地處理，包括可實現之資料主體權利以及有效之法律救濟，包括在歐盟內或第三國獲得有效的行政或司法救濟並請求補償。該等適當保護措施尤應符合個人資料處理之基本原則及設計與預設資料保護之原則。移轉之執行亦得由第三國之公務機關或公務機構向第三國之公務機關或公務機構或具對應責任或功能之國際組織為之，包括在規範基礎上加入諸如同意備忘錄、提供資料主體可執行且有效權利等行政安排。保護措施係以不具法拘束力之行政安排所提供者，應獲得有關監管機關之授權。

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract,

such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(109) 控管者或處理者使用執委會採用或監管機關採用之定型化資料保護條款的可能性，應避免控管者或處理者將定型化資料保護條款擴張適用於更廣泛之契約，例如處理者與其他處理者間之契約，亦應避免以增訂其他條款或額外保護措施而直接或間接牴觸執委會或監管機關所採用之定型化契約條款，或侵害資料主體之基本權或自由。控管者與處理者應被鼓勵透過補充定型化保護條款之契約上承諾來提供額外保護措施。

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(110) 企業集團或從事聯合經濟活動之企業團體就其從歐盟境內至相同團體組織內所為之國際移轉，應得使用經核准且具拘束力之企業守則，但以該等企業守則包括所有核心原則及可實現之權利以確保資料移轉或其分類設有適當保護措施者為限。

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation

to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(111) 於資料主體已明確同意時，以及於移轉基於契約或法律上主張之必要而不具經常性時，不問係於訴訟、行政程序或任何法庭外程序，包括管制機構前之程序，關於特定情況下移轉資料有其可能性之規定應予制定。在基於歐盟法或會員國法所訂定之重要公益理由要求時，或該移轉係來自法定登記且係為公眾或具正當利益之私人進行查詢時，關於移轉資料有其可能性之規定亦應予制定。在後者之情形，該移轉不應涵蓋全部之個人資料或該登記所涉及之全類別所含之全部資料，且當該登記係為有正當利益之私人進行查詢時，移轉應僅在其請求下進行，或若其為接收者，應完整考量資料主體之利益與基本權。

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of

contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(112) 該等例外尤應適用於受要求且基於公共利益之重要理由而有必要之資料移轉，例如國際間主管機關、稅務或關務機關間、金融監管機關之間、社會安全或公共衛生服務專責機關間之資料交換；例如傳染病之接觸追蹤或為了降低並 / 或消除藥物濫用之情形。若資料主體無法給予同意，於有必要保護資料主體之重要利益或其他人之重要利益，包括身體完整性或生命時，個人資料之移轉亦應被視為合法。在欠缺有充足保護程度之決定時，歐盟法或會員國法可能基於公共利益之重要理由，明確限制特定類別之資料移轉至第三國或國際組織。會員國應向執委會通知此種規定。任何於資料主體身體上或法律上無能力給予同意下所為之個人資料移轉至國際人道組織，按照完成目前在日內瓦公約之任務或遵循於武裝衝突時所適用之國際人道法的觀點，可以被視為必要的公共利益之重要理由或因為其屬於資料主體

之重要利益。

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(113) 當移轉係控管者為實現重大正當利益，且該利益並未劣後於資料主體之利益或權利及自由，並且該控管者已評估有關該資料移轉之所有情況者，合乎不具反覆性且僅涉及有限人數之資料主體之移轉亦屬可行。該控管者應特別考量個人資料之性質、所提議單一或多個處理活動之目的及持續期間以及起源國、第三國與最終目的地國之狀況，且應就該等個人資料處理提供適當保護措施，以確保當事人之基本權及自由。該等資料移轉應僅在其無其他得適用之合法性基礎之其餘案例上始有適用之可能。為科學或歷史研究目的或統計目的，社會知識增長之合理期待應被納入考量。控管者應將該移轉通知監管機關及資料主體。

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(114) 在任何情況下，於執委會尚未作成第三國關於資料處理有充足保護程度之決定時，一旦在歐盟境內所處理之資料已被移轉，控管者或處理者應設法提供資料主體可實現且有效之權利，使其等能繼續享有基本權及保護措施之利益。

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(115) 有些第三國會採用旨在直接規範個人或法人在會員國管轄權內所為處理活動之法律、規則或其他法令。此可能包括第三國之法院或法庭之判決或行政機關之決定要求控管者或處理者移轉或揭露個人資料，而其並非基於如司法互助條約等在要求資料

之第三國與歐盟或會員國間之國際協議。該等法律、規則及其他法令對於治外法權之適用可能違反國際法，且可能妨礙本規則達成對個人在歐盟之保護。移轉應僅得在本規則對於移轉至第三國所規定之條件皆成就時始被允許。此包括但不限於發生在揭露係基於歐盟法或會員國法所承認之公共利益的重要理由而控管者受該法之拘束且有必要之情形。

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(116) 當個人資料跨境移動至歐盟境外時，個人行使資料保護權利之能力處於更高的風險中，特別是保護其免於資料遭不法使用或揭露之能力。同時，監管機關可能發現其無法進行追訴或就境外活動實施相關之調查。其等在跨國之脈絡下合作之努力可能

面臨預防或矯正權力之不足、法制度不一致性及諸如資源限制等實務上之障礙。因此，有必要促成資料保護監管機關間更緊密之合作，以協助其等交換資訊並與其在國際上對應之部門共同進行調查。為了發展國際合作機制之目的以促進並提供執行個人資料保護法案之國際互助，基於對等原則並依據本規則，執委會及監管機關於行使其權力之有關行動中應與第三國之主管機關交換資訊及合作。

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(117) 在會員國內設立監管機關，並授權該機關有完全之獨立性來執行其任務及行使其權力，係對於個人資料處理保護之基本要素。會員國應得設立一個以上之監管機關，以反映其憲法、組織及行政架構。

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(118) 監管機關之獨立性不應代表監管機關不得成為有關其財務支出之控制或監督機制或司法審查之對象。

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism,

to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(119) 會員國設立數個監管機關者，應以法律為之，以確保各監管機關得在一致性機制下有效參與。為使各監管機關在該機制中得有效參與，會員國應特別指定一監管機關作為單一聯絡對口，以確保與其他監管機關、歐洲資料保護委員會及執委會間迅速且順暢之合作。

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(120) 為有效執行監管機關之任務，包括與遍佈全歐盟境內之其他監管機關相關互助與合作之該等任務，監管機關應被提供其所需之財務與人力資源、辦公室及基礎設施。各監管機關應有單獨、公開之年度預算，並可作為國家或聯邦整體預算之一部份。

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful

or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(121) 關於監管機關成員之一般性規範，應由各會員國以法律定之，並應特別規定該等成員係基於政府、政府成員、國會或國會議院或會員國立法委託之獨立機構之提案，依透明之程序選任，不問係由國會、政府或會員國之元首為之。為確保監管機關之獨立性，其成員應依誠信原則為各項行為，避免任何與其職務在性質上不相容之行為，且不應在其任期中從事任何性質上不相容之工作，不問該工作是否受有報酬。監管機關應擁有由監管機關或依會員國法設立之獨立機構所挑選出之職員，該等職員應遵從監管機關成員排他之行政指揮。

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(122) 各監管機關應有權限在其所屬會員國境內行使權力及執行其依據本規則被賦予之任務。此尤應涵蓋控管者或處理者之分支機構在該會員國境內所為之資料處理活動、公務機關或私人符合

公共利益所為之個人資料處理、在該國境內對資料主體造成影響之資料處理或非設立於歐盟境內之控管者或處理者對居住在其領土之資料主體執行之資料處理。此應包括受理資料主體所提出之申訴、就本規則之適用進行調查及加強公眾對個人資料處理相關風險、規範、保護措施及權利之認知。

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(123) 監管機關應依照本規則監督各條款之適用，並致力於確保本規則在全歐盟適用之一致性，以保護當事人關於其個人資料處理，並促進個人資料在歐洲市場之自由流通。為達該目的，監管機關相互間及其與執委會間應彼此合作，無須會員國間簽訂互助或該等合作條款之任何協議。

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the

territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(124) 凡個人資料之處理係由控管者或處理者於歐盟境內之分支機構所為，且該控管者或處理者在一個以上之會員國設立分支機構，或凡資料處理係由控管者或處理者在歐盟境內之單一分支機構所為，而該處理顯然影響或可能顯然影響一個以上會員國之資料主體者，該控管者或處理者之主要分支機構或該單一分支機構之監管機關應擔任領導機關之角色。因控管者或處理者在該會員國境內設有分支機構、或因居住於該會員國境內之資料主體受到影響，或因已對該會員國之監管機關提出申訴時，該領導機關應與其他相關機關合作。當資料主體並非居住於某會員國，而對該國之監管機關提出申訴者，該監管機關亦應屬相關監管機關。在委員會所負頒佈能涵蓋本規則適用所生任何疑義之指導原則的任務中，其應得特別在考量因素之判斷標準上頒佈指導原則，以確認該資料處理是否顯然影響一個以上會員國之資料主體，以及何者能構成相關且合理之異議。

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process.

Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(125) 關於執行依本規則所授予之權力的措施，領導機關應有權限通過有拘束力之裁決。在身為領導機關之資格下，監管機關應於裁決過程中密集參與並協調相關監管機關。當該裁決係全部或部分駁回資料主體之申訴時，受理該申訴之監管機關即應採納該裁決。

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(126) 該裁決應經領導監管機關及相關監管機關共同同意，且應係直接針對控管者或處理者之主要分支機構或單一分支機構，並對該控管者或處理者發生拘束力。控管者或處理者應採取必要之措施來確保本規則之遵循，及領導監管機關對於控管者或處理者之主要分支機構關於歐盟境內資料處理所為裁決之執行。

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such

cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(127) 當控管者或處理者設立於一個以上會員國之分支機構，但特定資料處理之標的僅涉及於單一會員國境內所為之處理，且僅涉及該單一會員國境內之資料主體時，例如，涉及在某一會員國之特定勞雇環境下之受雇者的個人資料時，非作為領導監管機關之各監管機關應有權限處理該等當地案件。在該等案件中，監管機關應將該案件通知領導監管機關，不得遲延。領導監管機關於受通知後，應決定是否由其依照領導監管機關及其他相關監管機關間合作之相關規範來處理該案件（即「單一窗口機制」），或係由為通知之監管機關以當地層級來處理該案件。在領導監管機關決定是否將由其處理該案件時，其應考量在為通知之監管機關所屬之會員國境內是否有控管者或處理者之分支機構，以確保對於控管者或處理者所為之裁決能有效施行。當領導監管機關決定處理該案件時，應給予為通知之監管機關

有提交裁決草案之機會，而應由領導監管機關在單一窗口機制下準備其裁決草案時盡最大程度考量之。

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(128) 有關領導監管機關及單一窗口機制之規範不應適用於公務機關或私人基於公共利益所為之資料處理的情形。在該等案件中唯一有權限行使依本規則所授予之權力的監管機關，應係該公務機關或私人設立所在會員國之監管機關。

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case,

respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(129) 為確保本規則於歐盟境內一致之監督及執行，監管機關於各會員國境內應有相同之任務及有效之權力，尤其在當事人之申訴案件中，應有包括調查之權力、矯正及制裁之權力，以及批准及建議之權力，且對於檢察機關在會員國法所擁有之權力不生影響，而應將本規則之違反檢送至司法機關並參與法律程序。該等權力亦應包括對資料處理課予一暫時或終局之限制，包括禁令。會員國得具體化其他依照本規則所定與個人資料保護有關之任務。監管機關之權力行使應依歐盟法及會員國法所定適當之程序性保護措施於合理期限內公平、公正為之。尤其，每個措施應具備適當性、必要性及比例性，以確保本規則之遵循、考量個別案件之情況，並尊重任何人在對其有不利影響之任何個別措施被實施前有請求聽審之權利，且避免對該人造成無謂之花費及過度之不便。進入處所之調查權應依照會員國程序法之特別規定為之，例如事先取得司法授權之要求。監管機關所

為具法律拘束力之各措施皆應以書面為之，且應明確清楚，並指出做成該措施之監管機關名稱、日期、首長或其授權之監管機關成員之署名以及為該措施之理由，並敘明有尋求有效救濟之權利。此不應排除依據會員國程序法所規定之額外要求。通過一個具法律拘束力之裁決意味著其可能引起作成該裁決之監管機關所在會員國的司法審查。

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(130) 當受理申訴之監管機關並非領導監管機關時，領導監管機關應依照本規則所定合作及一致性之相關規範，與受理申訴之監管機關緊密合作。在該等案件中，當欲採取產生法律效果之措施，包括處以行政罰鍰時，領導監管機關應盡可能考量受理申訴且應保有權限在其所屬會員國境內進行調查之監管機關的立場，並與該管監管機關保持聯繫。

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does

not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(131) 當有另一監管機關應就控管者或處理者之資料處理活動擔任領導監管機關，但申訴之具體標的或可能之違法行為僅涉及到該控管者或處理者在受理申訴或所調查出可能違法行為所在會員國之處理活動，且該標的並不會或較無可能對其他會員國之資料主體造成重大影響時，該受理申訴或查得或由其他管道得知疑似有違反本規則情況之監管機關應與該控管者尋求友好解決，若證實前述為不可行時，則應行使其完整之權力。此應包括：在該監管機關所屬會員國境內或就該會員國境內之資料主體所為之特定資料處理；在提供商品或服務的情況下特別針對該監管機關所屬會員國境內之資料主體所為之資料處理；或應以會員國法所課予之相關法律義務進行評估之資料處理。

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(132) 監管機關對公眾所為喚起公眾意識之活動應包括針對控管者或處理者之特定措施，包括微型及中小型企業以及個人，特別是

於教育之脈絡下。

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(133) 監管機關在執行任務時應互相協助，以確保本規則於歐洲市場間一致之適用與執行。監管機關要求互助，而在另一監管機關收到其要求後一個月內未予回應時，該監管機關得採用暫時性的措施。

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(134) 各監管機關應適時與其他監管機關聯合作業。受要求之監管機關應有義務於指定時間內回應之。

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(135) 為確保本規則能在歐盟境內一體適用，一個能讓監管機關間合

作之一致性機制應予建立。當資料處理活動會對數個會員國內眾多之資料主體產生影響，而監管機關試圖採取旨在產生法律效果之措施時，該機制尤應適用。當任何相關監管機關或執委會要求標的應於該一致性機制下處理時，亦應適用該機制。該機制不得損及執委會行使條約所賦予之權力時可能採取之任何措施。

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(136) 當適用一致性機制時，若委員會之多數成員皆如此決定，或任何相關監管機關或執委會如此要求者，該委員會應於一定時間內公告其意見。當監管機關間有爭執時，委員會亦應有權通過有法拘束力之裁決。為達該目的，原則上經其成員三分之二以上之多數決同意，其即應對監管機關間存有意見衝突之清楚特定案件，發布具法拘束力之裁決，尤其是在領導監管機關與相關監管機關間在協作機制下就個案所持見解，特別是就是否違反本規則之見解發生衝突時。

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt

duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(137) 為保護資料主體之權利及自由，特別是當存在之危險可能使資料主體之權利行使受到相當之阻礙者，實有急迫需求即刻行動。因此，監管機關應能夠在其境內採取充分且正當之暫時性措施，該措施應有明確之有效期限，且不得超過三個月。

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross- border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(138) 當監管機關意圖使某措施產生法律效果，於適用該機制為強制之情形，是否適用該機制應為該措施是否合法之條件之一。在其他跨境相關之案件中，領導監管機關與相關監管機關間之協作機制應予適用，且該等監管機關間之雙方或多方互助及共同合作在未啟動一致性機制之情況下亦可能被實行。

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection

Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(139) 為促進本規則之一體適用，委員會應被設立為歐盟之獨立機構。為達成此目的，委員會應有法人格地位。委員會應以其主席為代表。其應取代歐盟指令 95/46/EC 所設立之個人資料處理保護小組。其組成應包括各會員國監管機關及歐盟資料保護監管機關之首長或其等之相應代表。執委會應參與委員會之活動，但無表決權，且歐盟資料保護監管機關應有特別表決權。委員會應致力於本規則在歐盟境內適用之一致性，包括給予執委會建議，尤其是在第三國或國際組織之保護程度，並且應促進全歐盟各監管機關間之合作。委員會在執行其任務時，應獨立行使職權。

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(140) 委員會應由歐盟資料保護監管機關所提供之秘書協助之。有參與執行本規則授權予委員會之任務的歐盟資料保護監管機關職員僅得在委員會主席之指示下執行其任務，並應向委員會主席報告。

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject

considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(141) 各資料主體，尤其是在其經常居住之會員國境內，應有向個別監管機關提出申訴之權利，且於資料主體認為其依據本規則之權利受到侵害或監管機關對其申訴不予作為、部分或全部不受理或駁回或監管機關應作為以保護資料主體之權利而不作為時，應有依憲章第 47 條受有效司法救濟之權利。監管機關應在受司法審查下就申訴進行調查至對於該特定案件適當之程度。監管機關應在合理期間內通知資料主體就其申訴調查之程序及結果。若該案件需要進一步之調查或須與另一監管機關合作，其間之資訊應提供予資料主體。為使申訴之提出能順利進行，各監管機關應採取措施，如提供能以電子格式填具之申訴提交表格，且亦不排除其他溝通管道。

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field

of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(142) 當資料主體認為其依本規則所享有之權利受到侵害時，其應有權利委任依會員國法合法設立、以公益為目的，且在個人資料保護領域活躍之非營利機構、組織或社團，代理其向監管機關提出申訴、代理該資料主體行使司法救濟之權利，或於會員國法有規定時，代理其行使收受賠償金之權利。會員國得賦予該等機構、組織或社團在該會員國境內享有受資料主體委任獨立提出申訴之權利，以及在有理由認為資料主體之權利因違反本規則之個人資料處理而受有損害時，進行有效司法救濟之權利。惟該等機構、組織或社團得不被允許依資料主體之授權而獨立代表資料主體請求賠償。

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern

to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

(143) 任何自然人或法人皆有權利對委員會裁決依歐洲聯盟運作條約第 263 條向歐盟法院提起裁決無效之訴。作為該等裁決之相對人，如相關監管機關欲對之提出異議者，應依照歐洲聯盟運作條約第 263 條規定，於收受通知之兩個月內提起之。當委員會之裁決係直接且個別涉及於控管者、處理者或申訴人，依歐洲聯盟運作條約第 263 條規定，後者得在裁決於委員會網站上公布之兩個月內，提起裁決無效之訴。自然人或法人就監管機關對其作成有法律效果之裁決應得向該管會員國法院尋求有效司法救濟，且不影響其依歐洲聯盟運作條約第 263 條所享有之權利。該裁決尤其涉及監管機關調查、矯正及授權之權力行使，或申訴之不受理或駁回。然而，受有效司法救濟之權利並不包

含監管機關所採取之不具法律拘束力之措施，例如監管機關公告之意見或提出之建議。對監管機關之訴訟應對監管機關設立地之會員國法院提起之，且須依照該會員國程序法之規定進行。此等法院應行使完整之審判權，包括應審理與爭議有關之一切事實上及法律上問題。

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

當申訴遭監管機關不予受理或駁回時，申訴人得在該會員國之法院提起訴訟。在本規則有關司法救濟適用之脈絡下，當該國法院認為有必要對訟爭之裁決作出裁判時，其得請求歐盟法院就歐盟法（包括本規則）之解釋做成初步裁決，或於有歐洲聯盟運作條約第 267 條之情形時，其應請求之。再者，當監管機

關所執行之委員會裁決在該國法院被提起訴訟，且該委員會裁決之效力存有爭議時，該國法院並無宣布委員會之裁決無效之權力，但若其認該裁決無效時，應依照歐盟法院對歐洲聯盟運作條約第267條所為之解釋將該有效性之疑義提交至歐盟法院。然而，當委員會裁決有效性之爭議係由有機會對該裁決提起無效訴訟之自然人或法人所提出，尤其是當該裁決直接且個別對其生效，但其並未依歐洲聯盟運作條約第263條所定期間內提出者，該國法院不得將該爭議提交至歐盟法院。

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(144) 當受理監管機關裁決訴訟案件之法院有理由相信有關於同一資料處理之該等訴訟已於該會員國境內之其他有權管轄法院提起者，例如資料處理之控管者或處理者相同，或有相同之原因事實時，法院應與另一法院聯繫，以確認該等相關訴訟是否存在。若有相關訴訟繫屬於其他會員國法院者，先受理該案件之法院以外之其他任何法院得停止訴訟程序，或得依照訴訟當事人一

方之聲請，於先受理之法院對於系爭訴訟有管轄權且該國法律允許相關訴訟之合併時，由先受理該案件之法院優先管轄該案件。當數個訴訟緊密關聯，且共同審理及裁判較為有利且可避免因個別審理造成之裁判歧異者，該數訴訟視為相關。

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(145) 對控管者或處理者所提起之訴訟，原告應有權選擇在控管者或處理者之分支機構所在會員國法院或在資料主體居所地之法院起訴，但控管者係會員國行使其公權力之機關者，不在此限。

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller

or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(146) 控管者或處理者應賠償當事人因其違反本規則之資料處理所受之一切可能損害。若控管者或處理者能證明其從任何方面而言皆非造成損害之原因，則應免除其責任。損害之概念應依照歐盟法院之判例，以能完全反映本規則所欲達成之目標作較寬鬆之解釋。惟此不應損及就違反歐盟法或會員國法所定其他規則所生損害為任何主張之權利。違反本規則之資料處理，亦包括資料處理違反依據本規則所制定之授權法及施行法以及違反為具體化本規則之會員國法者。資料主體就其等所受損害，應受到充分且有實益之賠償。當控管者或處理者亦參與同一資料處理時，應追究各控管者或處理者就整個損害之法律責任。然而，當其等參與同一司法程序時，依據會員國法，在確保受到損害之資料主體能受到充分且有實益之賠償的前提下，可能依據各控管者或處理者就該資料處理造成損害結果之歸責程度進行損害賠償責任之分擔。任何負擔全部損害賠償責任之控管者或處理者，得續而展開對其他亦參與同一處理程序之控管者或處理者之追償程序。

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council[13] should not prejudice

[13] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil

the application of such specific rules.

(147) 凡本規則定有管轄權之特別規定者，尤其是關於對控管者或處理者請求包含損害賠償之司法救濟的資料處理時，諸如歐洲議會及歐盟理事會所定歐盟規則第 1214/2012 號 [13] 等之一般性司法規範不應損及該等特別規定之適用。

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(148) 為強化本規則之執行，對於本規則之任何違反，應被處以包括行政罰鍰等處罰，此不問係外加於監管機關依照本規則實施之適當措施，或取代該等措施。在僅有輕微之違反，或欲處以之

---

and commercial matters (OJ L 351, 20.12.2012, p. 1).
歐洲議會及歐盟理事會於 2012 年 12 月 12 日就民事及商事事件判決之管轄權、承認及執行制定歐盟規則第 1214/2012 號（官方公報 L 類第 351 期，2012 年 12 月 20 日，第 1 頁）。

罰鍰會造成對當事人不相當之負擔，得採用告誡之方式取代罰鍰。然而，仍應就該違反之性質、嚴重性、持續期間、是否為故意、有無降低損害之行為、責任程度或先前任何相關違反之程度、監管機關知悉其違法行為後之態度、命控管者或處理者所為措施之遵循、對行為守則之遵守以及有無任何使之加重或減輕之因素，為相當之考慮。實施包括行政罰鍰之處罰，應遵循歐盟法及憲章一般法律原則之適當程序保障，包括有效之司法保護及正當程序。

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(149) 會員國應得就本規則之違反，包括依本規則規定及在其所為限制範圍內所定內國法規定之違反，擬定刑罰規範。該等刑罰亦得允許沒入違反本規則所獲之利益。然而，對該等內國規範之違反所處以之刑罰及行政罰不應造成依歐盟法院所闡釋之「一事不再理原則」之違反。

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of

the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(150) 為強化及協調違反本規則所處以之行政罰，各監管機關應有權力處以行政罰鍰。本規則應指出何者構成違反，以及相關行政罰鍰的上限及裁罰基準，此應由每個個案中之主管監管機關決定之，並考量該個案情形所有相關之情狀，並適當考量該違反之性質、嚴重性及持續期間及其後果，及確保遵循本規則所定義務所採取之措施及預防或減輕該違反所造成之後果。對企業處以行政罰時，企業應被依照歐洲聯盟運作條約第 101 條及第 102 條所定義之目的為理解。對個人而非企業處以行政罰時，監管機關在考量適當之罰鍰金額時，應考量該會員國之平均所得，以及該個人之經濟狀況。一致性機制亦得被運用，以促使行政罰鍰適用之一致性。此應由會員國決定是否得對公務機關處以行政罰，以及至何程度。處以行政罰或給予警告並不影響監管機關其他權力之行使，或本規則下其他處罰之實施。

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(151) 丹麥及愛沙尼亞之法律體系不允許本規則所規範之行政罰鍰。行政罰之規範在丹麥得以該國管轄法院裁判處以刑罰之方式行之；在愛沙尼亞得以監管機關處理輕罪程序之架構處以罰金之方式行之；惟上開會員國該等規範之適用，應與監管機關處以罰鍰之效果相當。因此，內國管轄法院應考慮監管機關處以罰鍰之建議。在任何情況下，處以罰鍰應係有效、適當且具懲戒性的。

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(152) 當本規則未就行政罰鍰定有一致規範，或在其他案件中有必要者，例如嚴重違反本規則之情況時，會員國應採用有效、適當及懲戒性處罰之制度。此等處罰屬刑事或行政性質，應由會員國法律決定之。

(153) Member States law should reconcile the rules governing freedom of

expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(153) 會員國法應依照本規則調和包括新聞、學術、藝術及或文學表達等表意自由與資訊自由與個人資料保護之權利。在必須調和個人資料受保護權利與表意與資訊自由時，依憲章第 11 條之意旨，專為新聞、學術、藝術或文學表達目的所為之個人資料處理，應得除外於或豁免於本規則之特定規定。此尤應適用於視聽領域、新聞檔案及媒體資料庫之個人資料處理。因此，會員國應採取擬定豁免或例外規定之立法措施，以達到平衡該等基

本權之目的。對於總則性規範、資料主體之權利、控管者及處理者、個人資料移轉至第三國或國際組織、獨立監管機關、合作和一致性、以及特定資料處理情形，會員國得訂定豁免或例外規定。當會員國之該等豁免或例外規定彼此不同時，控管者所受拘束之會員國法律應予適用。為考量每個民主社會中表意自由權利之重要性，與此自由相關之概念應給予較寬鬆之解釋，例如新聞業。

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council[14] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation.

---

[14] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).
歐洲議會及歐盟理事會於 2003 年 11 月 17 日就公部門訊息之再利用制定歐盟指令第 2003/98/EC 號（官方公報 L 類第 345 期，2003 年 12 月 31 日，第 90 頁）。

In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(154) 適用本規則時，本規則允許考量公眾取得政府文件之原則。公眾取得政府文件得被認為符合公共利益。於揭露係依照該機關或機構所受拘束之歐盟法或會員國法所為者，公務機關或公務機構所持文件上之個人資料應得由該機關或機構向大眾揭露。該等法律應調和公眾取得政府文件及公部門資訊之再利用，與依本規則保護個人資料之權利，因此可能依照本規則就個人資料保護之權利為必要之折衷。在此脈絡下之公務機關或公務機構應包括關於公眾接近使用文件之會員國法下所涵蓋之一切公務機關或其他機構。歐洲議會及歐盟理事會之歐盟指令第2003/98/EC 號 [14] 維持不變，且不影響歐盟法或會員國法對於個人資料處理保護之程度，尤其不改變本規則所規定之義務及權利。尤其，該指令不應適用於按制度以個人資料保護為由所被排除或被限制接近使用之文件，以及按制度所取得之部分文件，包括法律所規定與自然人個人資料處理保護互斥之個人資料的再利用。

(155) Member State law or collective agreements, including ‘works agreements’, may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid

down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(155) 會員國法或團體協約，包括「勞動協議」，得提供關於僱傭關係下員工個人資料處理之特別規定，尤其是當僱傭關係下個人資料處理可能係基於下列理由，亦即，包括員工之同意、為徵才目的、包括履行法律或團體協約所規定之義務等之僱傭契約之履行、工作之管理、計畫及或組織、工作場所之平等與多元性、工作之健康與安全、個人或團體與僱傭有關之權利及福利之行使及享有之目的，以及終止僱傭關係之目的。

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications

and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(156) 為符合公共利益、達成科學或歷史研究目的或統計目的所為個人資料之處理應受本規則為資料主體之權利或自由所定適當保護措施之拘束。該等保護措施應確保已備妥技術上及組織上之措施，用以確保，特別是資料最少蒐集原則之落實。為符合公共利益、達成科學或歷史研究目的或統計目的，當控管者已評估實現該等目的之可行性，且藉由不允許或不再允許識別資料主體為該處理，並有適當的保護措施存在（例如，資料之假名化）時，個人資料將得進行進階處理。會員國對於為達成公共利益目的之個人資料處理，應提供適當之保護措施。在進行符合公共利益、達成科學或歷史研究目的或統計目的之個人資料處理時，會員國在符合特定條件且有提供資料主體適當保護措施時，應有權具體化及除外化關於資訊之要求，以及關於更正、刪除、被遺忘、限制處理、資料可攜性及拒絕之權利。若依照特定資料處理所追求之目的為適當，且其技術上及組織上之措施係為落實適當性及必要性原則而減少個人資料處理時，其條件及保護措施可能需要有特定程序使資料主體得行使該等權利。

為科學目的之個人資料處理亦應遵守其他相關之法規，例如對於臨床試驗之規範。

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(157) 藉由結合資料庫之資訊，研究者得取得普遍醫療條件下高價值之新知識，例如心血管疾病、癌症及抑鬱症。當有更多的人口數時，在資料庫之基礎上，研究結果可被提升。在社會科學中，以資料庫為基礎之研究使研究者能取得關於取得數個社會條件之長期關連性基礎知識，例如失業及教育與其他生存條件之相關性。透過資料庫得出之研究結果提供堅實、高品質之知識，可作為依據知識形成政策之基礎，並增進一定數量之人之生活品質，以及促進社會服務之效能。為了促進科學研究，若依照歐盟法或會員國法所規定之適當條件及保護措施，可為科學研究目的而處理個人資料。

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public

authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(158) 當個人資料處理係為達成某些目的，本規則亦應適用於該處理，惟須特別注意本規則不應適用於死者。依照歐盟法或會員國法，持有公共利益紀錄之公務機關或公務機構或私人應有提供服務之法律義務，亦即有義務取得、保存、評估、安排、描述、溝通、促進、宣傳及提供對於一般公共利益有持久價值之記錄的存取。會員國亦應被授權規範為達成某些目的所為個人資料之進階處理，例如規範在早期極權主義國家政權、種族滅絕、納粹大屠殺等違反人類罪、或戰爭罪之下的政治行為之相關特定資訊。

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as

regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(159) 當個人資料係為科學研究目的而為處理，本規則亦應適用於該等資料之處理。為本規則之目的，對於為科學研究目的所為個人資料之處理應採較寬鬆之解釋，包括如科技發展及成果、基礎研究、應用研究及私人贊助之研究。此外，應考量歐盟在歐洲聯盟運作條約第 179 條第 1 項達成歐洲研究區域之目的。科學研究目的亦應包括為符合公共利益在公共衛生領域所進行之研究。為滿足處理個人資料用於科學研究目的之特殊性，尤其是關於出版或以其他方式在科學研究目的下揭露個人資料時，應適用特定之條件。若科學研究結果（尤其是在公共衛生領域者）為符合資料主體利益提供了進一步措施之理由，本規則之一般規定應適用該等措施。

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(160) 為歷史研究目的進行個人資料處理時，本規則亦應適用於該資料處理。此亦應包括歷史研究及家族史研究，尤應注意本規則不應適用於死者。

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council[15] should apply.

[15] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16

(161) 為同意參與臨床試驗科學研究活動之目的，歐洲議會及歐盟理事會之歐盟規則第 536/2014 號 [15] 應適用之。

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(162) 當為統計目的進行個人資料處理時，本規則應適用於該等資料處理。在本規則之限制範圍內，歐盟法或會員國法應決定統計內容、存取控制、對為統計目的之個人資料處理的詳述、以及保護資料主體權利與自由之適當措施，並確保統計機密性。統計目的係指任何蒐集活動以及統計調查或產生統計結果所必須之個人資料處理。此等統計結果可能進一步被用於不同的目的，包括科學研究目的。統計目的意味著為統計目的之資料處理結果不是個人資料，而係總體資料，且該結果或該個人資料並非

April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).
歐洲議會及歐盟理事會於 2014 年 4 月 16 日就人用藥品之臨床適用制定歐盟規則第 536/2014 號，取代指令第 2001/20/EC 號（官方公報 L 類第 158 期，2014 年 5 月 27 日，第 1 頁）。

用於支持關於任何特定當事人之措施或決定。

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council[16] provides further specifications on statistical confidentiality for European statistics.

(163) 歐盟及國家統計機關為產生歐洲官方及各國官方統計資料而蒐集之機密資訊應被保護。歐洲統計資料應依歐洲聯盟運作條約第 338 條第 2 項所定之統計原則為研製、製作及宣傳，但國家統計資料亦應遵守會員國法律。歐洲議會及歐盟理事會之歐盟規則第 223/2009 號 [16] 規定關於歐洲統計資料統計機密性之進一步細節。

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the

---

[16] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).
歐洲議會及歐盟理事會於 2009 年 3 月 11 日就歐洲統計資料，制定歐盟規則第 223/2009 號，取代歐洲議會及歐盟理事會第 1101/2008 號規則—依循歐洲共同體統計辦公室統計機密性之資料傳輸、歐盟理事會規則第 322/97 號—社區統計及歐盟理事會決議第 89/382/EEC 號—歐洲原子能共同體成立歐洲共同體統計計畫委員會（官方公報 L 類第 87 期，2009 年 3 月 31 日，第 164 頁）。

professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(164) 關於監管機關自控管者或處理者處取得個人資料及進入其等辦公處所之權力，在為調和個人資料保護權利與職業秘密之保密義務間必要之範圍內，會員國得在本規則限制之範圍內以法律具體化規範，以保護職業或其他相應之保密義務。此無損於會員國現存之義務，即當歐盟法有所要求時，應通過關於職業秘密規範之義務。

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(165) 如同歐洲聯盟運作條約第 17 條所揭示，本規則尊重且不損害各會員國現有憲法對教會及宗教組織或社團之規範狀態。

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant

documents to the European Parliament and to the Council.

(166) 為了實現本規則之目標，亦即保護當事人之基本權及自由，尤其是其個人資料受保護之權利，並確保個人資料在歐盟境內之自由流通，依照歐洲聯盟運作條約第 290 條規定通過法案之權力應授予執委會。尤其，關於認證機制之標準與要求、標準化圖示之資訊及提供該等圖示之程序皆應以授權法明定之。尤其重要的是執委會在準備作業的過程中應進行包括專家層級之適當諮詢。當準備及起草授權法時，執委會應確保對歐洲議會及歐盟理事會為同步、及時且適當之相關文件的傳輸。

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(167) 為確保本規則施行之一致狀態，實行之權力應在本規則規定時授權予執委會。此等權力應依照歐盟規則第 182/2011 號而為行使。在該脈絡下，執委會應考量微型及中小型企業之特定措施。

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(168) 檢驗程序應使用於控制者與處理者間及處理者相互間的定型化契約條款之施行法的採用；行為守則；認證之技術標準與機制；第三國、第三國內之領域或特定部門、或國際組織所應負之適當保護程度；標準保護條款；依照有拘束力之合作規範，控管者、處理者及監管機關間以電子方式資訊交換之格式及程序；互助；及監管機關間及監管機關與歐洲資料保護委員會間以電子方式資訊交換之安排。

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(169) 當有充足之證據顯示有第三國、第三國內之領域或特定部門、或國際組織無法確保充足程度之保護，且有急迫理由者，執委會應採取立即生效之施行法。

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(170) 於本規則之目標無法充分地由會員國達成，亦即確保當事人受到相當程度之保護，以及個人資料在歐盟境內之自由流通之目的，且行動之規模或效果等理由較可以在歐盟層次中被實現時，歐盟得依據歐盟條約第 5 條對於輔助原則之規定採取措施。依據該條所規定之比例性原則，本規則不得超出達成該目標所必

須採取之手段。

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(171) 本規則取代歐盟指令第 95/46/EC 號。於本規則施行日時正在進行之資料處理，應於本規則生效後兩年內使其符合本規則之規定。當資料處理係基於依據歐盟指令第 95/46/EC 號之同意時，若該資料主體表示之同意已符合本規則所定之條件者，其不須再次表示同意，以使控管者得於本規則施行後繼續為該資料之處理。執委會決議及監管機關依據歐盟指令第 95/46/EC 號之授權仍維持有效直到被修正、代替或取代。

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012[17].

(172) 歐盟資料保護監管機關依歐盟規則第 45/2001 號第 28 條第 2 項接受諮詢，並於 2012 年 3 月 7 日發表其意見 [17]。

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à- vis* the processing of personal data which are not subject to specific obligations with the

[17] OJ C 192, 30.6.2012, p. 7.
官方公報 C 類第 192 期，2012 年 6 月 30 日，第 7 頁。

same objective set out in Directive 2002/58/EC of the European Parliament and of the Council[18], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

(173) 本規則應適用於所有涉及保護個人資料處理之基本權及自由之事件，且不限於歐洲議會及歐盟理事會之歐盟指令第 2002/58/EC 號 [18] 為同樣目的所規定之特定義務，包括控管者之義務及當事人之權利。為釐清本規則與歐盟指令第 2002/58/EC 號之關係，該指令應依本規則修訂。一旦通過本規則，歐盟指令第 2002/58/EC 號應受檢討，尤其是為確保與本規則之一致性，

HAVE ADOPTED THIS REGULATION:

已施行本規則：

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

2002 年 7 月 12 日歐洲議會及歐盟理事會之歐盟規則第 2002/58/EC 號關於在電子通訊方面個人資料處理及隱私權保護（隱私及電子通訊指令）（官方公報 L 類第 201 期，2002 年 7 月 31 日，第 37 頁）。

CHAPTER I General provisions

第一章　總則

Article 1 Subject-matter and objectives

第一條　主旨與立法目的

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
1. 為規範關於保護個人資料處理與資料自由流通，特制定本規則。
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
2. 本規則保護個人基本權與自由，尤其是保護個人資料之權利。
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
3. 個人資料於歐盟境內之自由流通，不得以保護個人資料處理有關理由限制或禁止之。

Article 2 Material scope

第二條　實體適用範圍

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
1. 本規則適用於全部或一部以自動化方式處理之個人資料，且適用於其他非自動化方式處理而構成檔案系統之一部分或旨在構成檔案系統之一部分的個人資料。
2. This Regulation does not apply to the processing of personal data:
2. 下列個人資料處理，不適用本規則：

(a) in the course of an activity which falls outside the scope of Union law;

(a) 於歐盟法外治權領域之活動；

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(b) 由會員國所進行屬於歐盟條約第二章第 5 節範圍內之活動；

(c) by a natural person in the course of a purely personal or household activity;

(c) 當事人所為單純之個人或家庭活動；

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(d) 主管機關為達預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的（包括為維護及預防對於公共安全造成之威脅）所為之個人資料處理。

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

3. 歐盟規則第 45/2001 號適用於歐盟當局、機構、辦事處及局處所為之個人資料處理。歐盟規則第 45/2001 號及其他涉及個人資料處理之歐盟法案應依本規則第 98 條規定，按本規則之原則與規定調整修正之。

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

4. 本規則不得影響歐盟指令第 2000/31/EC 號之適用，特別是中介服務商依該指令第 12 至 15 條規定所負之義務。

Article 3 Territorial scope

第三條　領土適用範圍

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

1. 本規則適用於控管者或處理者在歐盟境內之分支機構所為之個人資料處理活動，不問該處理是否發生於歐盟境內。

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

2. 本規則適用於由非設立於歐盟境內之控管者或處理者對於歐盟境內之資料主體所為涉及如下事項之個人資料處理：

   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

   (a) 對歐盟境內之資料主體提供商品或服務，不問是否需要資料主體付款；

   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

   (b) 對於資料主體於歐盟內所為行為之監控。

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

3. 本規則適用於由非設立於歐盟境內之控管者，但在會員國法律依國際公法可得適用領域內所為之個人資料處理。

Article 4 Definitions

第四條　定義

For the purposes of this Regulation:

為本規則之目的：

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

(1) 「個人資料」係指有關識別或可得識別自然人（「資料主體」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(2) 「處理」係指對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如收集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀。

(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(3) 「處理限制」係指對於已儲存之個人資料進行標記，以限制其未來之處理。

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal

aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(4) 「建檔」係指對個人資料任何形式之自動化處理，包括使用個人資料來評估與該當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵；

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(5) 「假名化」係指處理個人資料之方式，使該個人資料在不使用額外資訊時，不再能夠識別出特定之資料主體，且該額外資料已被分開存放，並以技術及組織措施確保該個人資料無法或無可識別出當事人。

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(6) 「檔案系統」係指依據特定標準可接近使用之個人資料所建構之任何檔案，不問是集中式、分散式或依功能性或地域性分散式之檔案。

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(7) 「控管者」係指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準；

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(8) 「處理者」係指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構；

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(9) 「接收者」係指個人資料被向其揭露之自然人或法人、公務機關、局處或其他機構，不問其是否為第三人。但依據歐盟法或會員國法律，在特定調查框架內可能接收個人資料之公務機關不應視為接收者；該等公務機關所為資料之處理，應依照其處理目的，遵守其所適用之資料保護規則；

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(10) 「第三人」係指資料主體、控管者、處理者及在控管者或處理者直接授權下被授權處理個人資料之人以外之自然人或法人、公務機關、局處或其他機構；

(11) 'consent' of the data subject means any freely given, specific,

informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(11) 資料主體之「同意」係指資料主體基於其意思，透過聲明或明確肯定之行動，所為自主性、具體、知情及明確之表示同意處理與其有關之個人資料；

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(12) 「個人資料侵害」係指違反安全性導致傳輸、儲存或以其他方式處理之個人資料遭意外或非法破壞、遺失、變更、未獲授權之揭露或接近使用；

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(13) 「基因資料」係指涉及當事人遺傳性或突變性之基因特徵之個人資料，尤其是經由當事人生物樣本分析後所取得關於該當事人獨特之生理或健康資訊；

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(14) 「生物特徵識別資訊」係指透過特定技術處理所得關於當事人身體、生理或行為特徵而允許或確認其特定識別性之個人資料，例如臉部圖像或診斷資料；

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(15) 「涉及健康之資料」係指與當事人之身體或精神健康有關之個人資料，包括提供揭示其健康狀況之醫療照顧服務；

(16) 'main establishment' means:

(16) 「主要分支機構」係指：

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(a) 於一個以上會員國內成立分支機構之控管者，其於歐盟境內核心管理機構之所在地，但個人資料處理的目的及方式係由控管者於歐盟境內另一分支機構所決定，且後者有權使其所為決定予以執行者，於此情形，作成該等決定之分支機構應被視為主要分支機構；

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(b) 於一個以上會員國內成立分支機構之處理者，其於歐盟境內核心管理機構之所在地，或如其於歐盟境內並無核心管

理機構時，歐盟為該處理者之分支機構之主要處理活動所在地，且該等活動使其須遵守本規則所規定之具體義務之處理者之分支機構；

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(17) 「代表」係指控管者或處理者依據第 27 條規定書面指定在歐盟境內之自然人或法人，而代表控管者或處理者依本規則各自所負之義務；

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(18) 「企業」係指從事經濟活動之自然人或法人，不問其法律形式，包括經常性從事經濟活動之合夥或組織；

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(19) 「企業集團」係指控制企業及其從屬企業；

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(20) 「有拘束力之企業守則」係指會員國境內成立之控管者或處理者，在企業集團內或從事於共同經濟活動之企業集團間，為移轉或一系列移轉個人資料至一個或多個成立於第三國之控管者或處理者所應遵守之個人資料保護政策；

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(21) 「監管機關」係指會員國依第 51 條規定成立之獨立公務機關；

(22) ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

(22) 「相關監管機關」係指因下列事由涉及之個人資料處理之監管機關：

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(a) 控管者或處理者係在該監管機關會員國境內成立；

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(b) 資料主體居住於該監管機關會員國境內，且受處理之實質影響或可能受到實質影響者；或

(c) a complaint has been lodged with that supervisory authority;

(c) 已向該監管機關提出申訴者；

(23) ‘cross-border processing’ means either:

(23) 「跨境處理」係指：

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(a) 歐盟境內之控管者或處理者在一個以上之會員國境內成立，而在一個以上之會員國之分支機構之活動過程中處理個人資料；或

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(b) 歐盟境內之控管者或處理者之單一分支機構之活動過程中

處理個人資料，但實質影響或可能實質影響到居住於一個以上會員國之資料主體；

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(24) 「相關且合理之異議」係指對於裁決草案關於是否有違反本規則之行為、或控管者與處理者有關之預設性行動是否符合本規則之判斷所為之異議，且該異議清楚證明裁決草案對於資料主體之基本權及自由及個人資料在歐盟境內自由流通（如適用）造成重大風險；

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

(25) 「資訊社會服務」係指歐洲議會及歐盟理事會[1]所定歐盟指令第2015/1535號第1條第1項第b點所定義之服務；

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

(26) 「國際組織」係指受國際公法管轄之組織及其附屬機構或依據

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).
歐洲議會及歐盟理事會於2015年9月9日為資訊社會服務規則領域及技術規則領域提供資訊之程序規定制定歐盟指令第2015/5135號（官方公報L類第251號，2015年9月17日，第1頁）。

兩個或多個國家所定協議成立或以此為基礎所成立之任何其他機構。

CHAPTER II Principles

第二章　原則

Article 5 Principles relating to processing of personal data

第五條　個人資料處理原則

1. Personal data shall be:

1. 個人資料應：

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(a) 為資料主體為合法、公正及透明之處理（「合法性、公正性及透明度」）；

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(b) 蒐集目的須特定、明確及合法，且不得為該等目的以外之進階處理；依照第 89 條第 1 項規定，為達成公共利益之目的、科學或歷史研究目的或統計目的所為之進階處理，不應視為不符合原始目的（「目的限制」）；

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(c) 適當、相關且限於處理目的所必要者（「資料最少蒐集原則」）；

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(d) 正確且必要時應隨時更新；考慮個人資料處理之目的，應採取一切合理措施，確保不正確之個人資料立即被刪除或更正（「正確性」）；

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(e) 資料主體之識別資料保存於一定形式，不長於處理目的所必要之期間；個人資料處理係單獨為達成公共利益之目的、科學或歷史研究目的或統計目的，且符合第 89 條第 1 項規定，實施適當之技術上及組織上之措施以確保資料主體權利及自由之要求者，該個人資料得被儲存較長時間（「儲存限制」）；

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(f) 處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理，並防止意外遺失、破壞或損壞（「完整性和保密性」）。

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').
2. 控管者應遵守並就其符合第 1 項規定負舉證責任（「責任」）。

Article 6 Lawfulness of processing

第六條 處理之合法性

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
1. 合法之處理應至少符合下列要件之一：
   (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   (a) 資料主體同意為一個或多個特定目的處理其個人資料；
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (b) 處理係為向身為契約當事人之資料主體履行契約所必須者，或在締約前，應資料主體之要求，所必須採取之步驟；
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   (c) 處理係控管者為遵守法律義務所必須者；
   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   (d) 處理係為保護資料主體或他人重大利益所必須者；
   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   (e) 處理係為符合公共利益執行職務或委託控管者行使公權力所必須者；
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such

interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(f) 處理係控管者或第三者為追求正當利益之目的所必須者，但該個人資料保護之資料主體之利益或基本權與自由優先於該等利益，特別是該資料主體為兒童時，不適用之；

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

第 1 款第 f 點不適用於公務機關執行其任務時所為之處理。

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

2. 會員國得維持或採用更具體之規範，使其與本規則所定本條第 1 項第 c 點及第 e 點之適用相符，為處理及用以確保處理合法性與公正性之其他措施，包括為第九章所規定之其他特定處理情形，訂定更具體化之特定規範。

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

3. 第 1 項第 c 點及第 e 點所定處理之依據應為：

(a) Union law; or

(a) 歐盟法；或

(b) Member State law to which the controller is subject.

(b) 控管者受拘束之會員國法律。

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

處理之目的應在該法律依據上被確立，或如第 1 項第 e 點所定之處理，應為符合公共利益執行職務或委託控管者行使公權力所必須者。該法律依據可能包含與本規則規定適用相符之具體規範，包括但不限於：規範控管者之個人資料處理合法性的一般條款；處理所涉及之個人資料之類型；相關資料主體；得向其揭露個人資料之主體及其目的；目的限制；儲存期間；及處理方式與處理程序，包括例如第九章所規定之其他特定處理情形，用以確保處理合法性與公正性之其他措施。歐盟法或會員國法律應符合公共利益之目標，並應與所追求之正當目標相適當。

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

4. 如處理係出於蒐集個人資料目的以外之目的且非基於資料主體同意，或非依據歐盟法或會員國法律在民主社會中為確保第 23 條第

1 項所定目的構成必要且適當方法所為時，控管者為確保處理之目的與原先蒐集個人資料之目的相互兼容應考慮包括但不限於下列事項：

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(a) 蒐集個人資料之目的與所欲進階處理目的間之任何連結性；

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(b) 蒐集個人資料之背景，尤其是資料主體與控管者間之關係；

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(c) 個人資料之本身性質，尤其是依據第 9 條特殊類型之個人資料處理，或依據第 10 條涉及前科及犯罪有關之個人資料處理；

(d) the possible consequences of the intended further processing for data subjects;

(d) 所欲進階處理對於資料主體造成之可能後果；

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(e) 適當保護措施之存在，可能包括加密或假名化。

Article 7　Conditions for consent

第七條　同意條件

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

1. 當處理係基於同意時，控管者應證明資料主體已同意其個人資料之處理。

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

2. 如資料主體之同意併係為其他事件所為之書面聲明時，同意請求應以易懂且方便取得之格式，並採用清楚簡易之語言，且與其他事件清楚區分之方式呈現。該聲明之任何條款違反本規則者，不具約束力。

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

3. 資料主體有權隨時撤回其同意。同意之撤回不影響撤回前基於該同意所為處理之合法性。資料主體為同意前，資料主體應受告知其得隨時撤回該同意。同意之撤回應與給予同意一樣容易。

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

4. 在評估同意之給予是否具自主性時，應特別考慮，包括但不限於，契約之履行（包括服務之提供）依存於個人資料處理之同意，且處理個人資料非履行契約所必要者。

Article 8 Conditions applicable to child's consent in relation to information society services

第八條　涉及資訊社會服務適用兒童同意之條件

1. Where point (a) of Article 6(1) applies, in relation to the offer of

information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

1. 第 6 條第 1 項第 a 點適用於直接向兒童提供資訊社會服務之情況，如兒童年滿 16 歲，兒童之個人資料處理應屬合法。如該兒童未滿 16 歲，僅限於其法定代理人授權或同意之範圍內，該等處理始為合法。

   Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

   會員國得以法律為該等目的規定較低年齡，惟不得低於 13 歲。

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
2. 在兒童之法定代理人授權或同意之情況，控管者應作出合理努力，在考量現有科技之情況下，確認該法定代理人之同意或授權。
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
3. 第 1 項規定不影響會員國之一般契約法，例如與兒童有關之契約之有效性、形成或效力之規定。

Article 9 Processing of special categories of personal data
第九條 特殊類型之個人資料處理

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be

prohibited.

1. 揭露種族或人種、政治意見、宗教或哲學信仰或貿易聯盟會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關個人資料之處理，應予禁止。

2. Paragraph 1 shall not apply if one of the following applies:

2. 有下列情形之一者，不適用第 1 項規定：

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(a) 除歐盟法或會員國法律規定資料主體不得排除第 1 項所定之禁止外，資料主體已明確同意為一個或多個特定目的處理上開個人資料；

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(b) 為履行義務及行使控管者特定權利之目的，或資料主體在歐盟法或會員國法或依據會員國法律所定適當保障資料主體之基本權及利益之團體協約所授權之勞動法及社會安全及社會保護法領域而有必要之處理；

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(c) 資料主體在身體上或法律上不能給予同意，而為保護資料主體或他人之重大利益所必要之處理；

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(d) 基金會、協會或任何其他非營利組織，基於政治、哲學、宗教或工會之目的，就其合法活動過程中所為之處理已做適當保護措施，且該處理僅涉及該組織之成員或其過去成員，或與該組織目的有關而定期接觸該組織之人，且該等個人資料未經資料主體之同意不會對外揭露者；

(e) processing relates to personal data which are manifestly made public by the data subject;

(e) 資料主體明顯已自行公開之個人資料之處理；

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(f) 為建構、行使或防禦法律上之請求或法院執行其司法權而有必要之處理；

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(g) 尊重資料保護之實質權利，並提供適當及具體之保護措施，以保護資料主體之基本權及利益，而基於歐盟法或會員國法律且與所追求目的合比例性之重大公共利益之理由所必要之

處理；

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(h) 依據歐盟法或會員國法律或基於與健康專業人員所定且受第3項要件及保護措施所拘束之契約，且為預防或職業醫學之目的、為評估僱員之工作能力、醫療診斷、為提供健康或社會照護或治療或為健康管理或社會照護系統及服務而有必要之處理；

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(i) 處理係基於公共衛生領域之公共利益，例如為防止對於健康之跨境嚴重威脅或為確保醫療保健及醫療產品或醫療設備品質之高標準與安全性而有必要者，並依據歐盟法或會員國法律規定採取適當及具體安全措施保護資料主體之權利和自由，尤其是職業秘密；

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and

provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(j) 尊重資料保護之實質權利，並提供適當及具體之保護措施，以保護資料主體之基本權及利益，基於歐盟法或會員國法律所定第 89 條第 1 項規定且與所追求目的合比例性者，為追求公共利益、科學或歷史研究目的或統計目的而有必要之處理；

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

3. 當資料係由基於歐盟法或會員國法或國內主管機構所訂定之規則受職業秘密之義務所拘束之專業人員或其他人處理或由其負責處理時，為第 2 項第 h 點所定目的，得處理第 1 項所定之個人資料；

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

4. 會員國得維持或採用進一步規定，包括但不限於關於基因資料、生物特徵識別資訊或與健康相關資訊之個人資料處理。

Article 10 Processing of personal data relating to criminal convictions and offences

第十條　涉及前科及犯罪之個人資料處理

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal

convictions shall be kept only under the control of official authority.
依第 6 條第 1 項處理涉及前科及犯罪之個人資料或相關安全措施，僅有下列情形之一者，始得為之：於公務機關控制下所為之處理，或歐盟或會員國法已為資料主體之權利與自由規範適當保護措施而授權之處理。任何全面性的前科紀錄僅限由公務機關控管保存。

Article 11 Processing which does not require identification
第十一條　不須識別之處理

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
1. 控管者處理個人資料之目的非為識別資料主體，或不再需要由控管者識別資料主體時，該控管者應無義務維護、取得或處理依照本規則以識別該資料主體為唯一目的之額外資訊。
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.
2. 本條第一項所定情形，如控管者得證明其非立於識別該資料主體之地位者，該控管者應於可能範圍內通知該資料主體。於此情形，第 15 條至第 20 條規定應不予適用，但資料主體依該等規定，為行使其權利之目的，提供得識別其身分之額外資訊者，不在此限。

CHAPTER III Rights of the data subject
第三章　資料主體之權利

Section 1 Transparency and modalities
第一節　透明度及管道

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject
第十二條　資料主體為行使其權利之透明資訊、溝通及管道

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

1. 控管者應採取適當措施，以簡明、透明、易懂且方便取得之格式，並採用清楚簡易之語言，提供第 13 條及第 14 條所定任何資訊及第 15 條至第 22 條及第 34 條所定關於對資料主體所為處理之任何溝通，特別是對於兒童之資訊。該資訊應以書面或其他方式提供，包括於適當情況下之電子格式。當資料主體提出要求，並以其他方式確認資料主體之身分者，得以口頭提供資訊。

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

2. 控管者應促使資料主體依照第 15 條至第 22 條規定行使其權利。於第 11 條第 2 項規定之情形，該控管者不應拒絕資料主體基於第 15 條至第 22 條行使其權利之要求，但該控管者證明其無從識別該資料主體之地位者，不在此限。

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

3. 控管者應向資料主體提供其依第 15 條至第 22 條提出之請求所欲採取行動之資訊，不得無故遲延，且無論如何，最遲應於收到請求後一個月內為之。考量到請求之複雜性及數量，該期限於必要時得再延長兩個月，控管者應於收到請求後一個月內通知資料主體該展期，並說明遲延之原因。資料主體以電子方式提出請求者，除資料主體另有要求者外，該資訊應盡可能以電子方式提供。

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

4. 如控管者不同意資料主體之要求者，該控管者應立即且最遲於收到資料主體要求之一個月內附具理由告知該資料主體，並敘明向監管機關提出申訴及尋求司法救濟之可能性。

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

5. 第 13 條及第 14 條所定應提供之資訊及第 15 條至第 22 條及第 34 條所定任何溝通及採取之任何行動，應無償提供之。如資料主體之請求明顯無理由或過度者，尤其是基於該等請求過於重複者，控管者得：

   (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

   (a) 考量所要求提供之資訊或溝通或採取行動之行政成本，收取適當費用；或

   (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

   (b) 拒絕該請求。控管者應就該請求之明顯無理由或過度性負舉證責任。

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

6. 在不影響第 11 條規定之情況下，如控管者對於當事人依照第 15 條至第 21 條提出請求之資料主體身分有合理懷疑者，控管者得要求提供為確認該資料主體身分所必要之額外資訊。

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.
7. 依據第 13 條及第 14 條規定提供予資料主體之資訊，得以標準化之標誌方式提供，俾提供易見、易懂且清晰易讀之方式，並對於所欲為之處理進行有意義之概述。於標誌係以電子方式表示時，其須得由機器辨認之。
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.
8. 依照第 92 條規定，為決定該等圖示所呈現之資訊及提供標準化圖示之程序之目的，執委會應有權通過授權法。

Section 2 Information and access to personal data
第二節　個人資料之資訊與接近使用

Article 13 Information to be provided where personal data are collected from the data subject
第十三條　蒐集資料主體之個人資料時所提供之資訊

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
1. 從資料主體蒐集其有關之個人資料時，控管者應於取得個人資料時，提供資料主體下列所有資訊：
   (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(a) 控管者及其代表（如適用）之身分及聯繫方式；

(b) the contact details of the data protection officer, where applicable;

(b) 資料保護員（如適用）之聯繫方式；

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(c) 所欲處理之個人資料之處理目的及該處理之法律依據；

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(d) 處理係依據第 6 條第 1 項第 f 點者，該控管者或第三人所追求之正當利益；

(e) the recipients or categories of recipients of the personal data, if any;

(e) 個人資料之接收者或接收者類型（如有）；

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(f) 控管者欲將個人資料移轉至第三國或國際組織，及執委會是否提供充足保護之決定，或於第 46 條或第 47 條或第 49 條第 1 項第 2 款所定傳輸之情形者，告知合適或適當之保護措施及取得該副本或該副本可得取用之方式（如適用）。

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

2. 除第一項所定資訊外，控管者於取得個人資料時，應提供資料主體下列必要之進階資訊，以確保公平及透明之處理：

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(a) 個人資料將被儲存之期間，或如告知期間不可能者，確定該期間所採用之標準；

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(b) 向控管者請求接近使用及更正或刪除或限制處理或拒絕處理與資料主體相關個人資料之權利，以及資料可攜性之權利；

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(c) 處理係依據第 6 條第 1 項第 a 點或第 9 條第 2 項第 a 點者，得隨時撤回其同意之權利，但不影響撤回前基於該同意所為處理之合法性；

(d) the right to lodge a complaint with a supervisory authority;

(d) 向監管機關提起申訴之權利；

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(e) 個人資料之提供是否為法定或契約要求，或係訂立契約之必要要件，以及資料主體是否有義務提供個人資料以及未提供該資料可能產生之後果；

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the

significance and the envisaged consequences of such processing for the data subject.

(f) 存在第 22 條第 1 項及第 4 項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

3. 如控管者所欲進階處理個人資料之目的非基於蒐集該個人資料之目的者，控管者在進階處理前，應提供資料主體該其他目的之資訊及第 2 項所定之任何相關進階資訊。

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

4. 第 1 項、第 2 項及第 3 項不適用於資料主體已有該資訊之內容及範圍。

Article 14 Information to be provided where personal data have not been obtained from the data subject

第十四條 尚未自資料主體取得個人資料時所應提供之資訊

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

1. 尚未自資料主體取得個人資料時，控管者應提供資料主體下列資訊：

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(a) 控管者及其代表（如適用）之身分及聯繫方式；

(b) the contact details of the data protection officer, where applicable;

(b) 資料保護員（如適用）之聯繫方式；

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(c) 所欲處理之個人資料之處理目的及該處理之法律依據；

(d) the categories of personal data concerned;

(d) 個人資料所涉及之類型；

(e) the recipients or categories of recipients of the personal data, if any;

(e) 個人資料之接收者或接收者類型（如有）；

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(f) 控管者欲將個人資料移轉至第三國或國際組織，及執委會是否提供充足保護之決定，或於第 46 條或第 47 條或第 49 條第 1 項第 2 款所定傳輸之情形者，告知合適或適當之保護措施及取得該副本或該副本可得取用之方式（如適用）。

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

2. 除第一項所定資訊外，控管者應提供資料主體下列必要之進階資訊，以確保對於資料主體為公平及透明之處理：

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(a) 個人資料將被儲存之期間，或如告知期間不可能者，確定該期間所採用之標準；

(b) where the processing is based on point (f) of Article 6(1), the

legitimate interests pursued by the controller or by a third party;

(b) 處理係依據第 6 條第 1 項第 f 點者，控管者或該第三人所追求之正當利益；

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(c) 向控管者請求接近使用及更正或刪除或限制處理或拒絕處理與資料主體相關個人資料之權利，以及資料可攜性之權利；

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) 處理係依據第 6 條第 1 項第 a 點或第 9 條第 2 項第 a 點者，得隨時撤回其同意之權利，但不影響撤回前基於該同意所為處理之合法性；

(e) the right to lodge a complaint with a supervisory authority;

(e) 向監管機關提起申訴之權利；

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(f) 個人資料之來源為何，及其是否來自可公開接近使用之來源 (如適用)；

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(g) 存在第 22 條第 1 項及第 4 項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。

3. The controller shall provide the information referred to in paragraphs 1 and 2:

3. 控管者應提供第 1 項及第 2 項所定資訊：

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(a) 在取得個人資料後之合理期間內，但最遲應於一個月內為之，須顧及個人資料處理之具體情形；

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(b) 如個人資料欲用於與資料主體之溝通，最遲於與該資料主體第一次溝通時；或

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

(c) 如預設會揭露予其他接收者時，最遲應於第一次揭露該個人資料時；

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. 如控管者所欲進階處理個人資料之目的非基於取得該個人資料時之目的者，控管者在進階處理前，應提供資料主體該其他目的之資訊及第 2 項所定之任何相關進階資訊。

5. Paragraphs 1 to 4 shall not apply where and insofar as:

5. 第 1 項至第 4 項不適用於：

(a) the data subject already has the information;

(a) 資料主體已有的資訊；

(b) the provision of such information proves impossible or would

involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(b) 經證明不可能提供該等資訊或須花費過鉅之勞費，尤其是為了實現公共利益、科學或歷史研究目的或統計目的，且符合第 89 條第 1 項所定要件及保護措施，或本條第 1 項所定義務可能使該處理目標無法實現或嚴重損害其實現者。於此情形，控管者應採取適當保護措施以保護資料主體之權利及自由及正當利益，包括公開資訊；

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(c) 取得或揭露係依據控管者所受拘束之歐盟法或會員國法律之明文，且歐盟法及會員國法律就保護資料主體合法利益之適當保護措施定有規範；或

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

(d) 如依照歐盟法或會員國法律所定專業保密義務之規範（包括法定之保密義務），個人資料應予保密者。

Article 15 Right of access by the data subject

第十五條　資料主體之接近使用權

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1. 資料主體有權向控管者確認其個人資料是否正被處理，於此情形者，資料主體應有權接近使用其個人資料及下列資訊：

(a) the purposes of the processing;

(a) 處理之目的；

(b) the categories of personal data concerned;

(b) 個人資料所涉及之類型；

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(c) 已揭露或將予揭露之個人資料接收者或接收者類型，尤其是在第三國境內或國際組織之接收者；

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(d) 如可能，個人資料將被儲存之預期期間，或如告知期間不可能者，確定該期間所採用之標準；

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(e) 向控管者請求更正或刪除或限制處理或拒絕處理與資料主體相關個人資料之權利；

(f) the right to lodge a complaint with a supervisory authority;

(f) 向監管機關提起申訴之權利；

(g) where the personal data are not collected from the data subject,

any available information as to their source;

(g) 個人資料非自資料主體蒐集所得者，關於該來源之任何充分資訊；

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(h) 存在第 22 條第 1 項及第 4 項所定自動決策（包括建檔）者，至少在該等情況，為資料主體之處理所涉及的邏輯性有意義資訊，以及重要性與預設結果。

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

2. 如個人資料移轉至第三國或至國際組織，該資料主體應有權獲知關於該傳輸依第 46 條所定之適當保護措施；

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

3. 控管者應提供所在處理之個人資料副本乙份。資料主體所要求之任何更多副本，控管者得依行政成本收取合理費用。如資料主體係以電子方式提出請求，除資料主體有不同要求外，該資訊之提供亦應以電子方式為之。

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

4. 第 3 項所定取得副本之權利不應影響其他人之權利及自由。

Section 3 Rectification and erasure
第三節　更正及刪除

Article 16 Right to rectification
第十六條　更正權

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

資料主體應有權使控管者更正其不正確之個人資料，不得無故拖延。考量到處理之目的，資料主體應有權完整化其有欠缺之個人資料，包括以提供補充說明之方式。

Article 17 Right to erasure ('right to be forgotten')
第十七條　刪除權（「被遺忘權」）

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1. 有下列情事者，資料主體應有權使控管者刪除其個人資料，不得無故拖延，且控管者應有義務刪除該個人資料，不得無故拖延：

   (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (a) 個人資料對於蒐集或處理目的不再需要者；

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(b) 處理係依據第 6 條第 1 項第 a 點或第 9 條第 2 項第 a 點者，資料主體撤回其同意，且該處理已無其他法律依據者；

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(c) 資料主體依第 21 條第 1 項規定對處理提出異議，且該處理無其他優先適用之法律依據者，或資料主體依第 21 條第 2 項規定對處理提出異議者；

(d) the personal data have been unlawfully processed;

(d) 該個人資料遭違法處理者；

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(e) 控管者依其受拘束之歐盟法或會員國法律有義務應刪除個人資料者；

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

(f) 個人資料係依據第 8 條第 1 項所定為提供資訊社會服務所蒐集者。

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

2. 如控管者已將該個人資料公開，且其有義務依據第 1 項規定刪除該個人資料者，考量現有科技及執行成本，該控管者應採取合理步驟，包括科技方式，通知正在處理該個人資料之控管者，資料

主體已提出刪去任何該個人資料之連結或複製或仿製之請求。

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

3. 於下列情形者，不適用第 1 項及第 2 項規定：

(a) for exercising the right of freedom of expression and information;

(a) 為行使表意自由及資訊權者；

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(b) 依據控管者所應遵守之歐盟法或會員國法，遵守其法律義務、或符合公共利益之職務執行、或委託控管者行使公權力所必須者；

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(c) 基於公共衛生領域上之公共利益，且符合第 9 條第 2 項第 h 點及第 i 點及第 9 條第 3 項規定者；

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(d) 為實現公共利益、科學或歷史研究目的或統計目的，且符合第 89 條第 1 項規定者，但以第 1 項所定權利實際上不可能或嚴重損害該處理目標之實現者為限；

(e) for the establishment, exercise or defence of legal claims.

(e) 為了建立、行使或防禦法律上之請求者。

Article 18 Right to restriction of processing

第 *18* 條　限制處理權

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

1. 於下列情事者，資料主體應有權限制控管者之處理：

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(a) 資料主體質疑其個人資料之正確性，而給予控管者驗證該個人資料正確性之期間；

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(b) 處理係違法的，且資料主體拒絕刪除該個人資料並要求限制其使用者；

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(c) 控管者就其處理之目的不再需要該個人資料，但該個人資料為資料主體建立、行使或防禦法律上請求所必須者；

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

(d) 資料主體已依照第 21 條第 1 項拒絕該處理，而在等待確認控管者是否具有優先於資料主體權益之正當理由；

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or

of a Member State.

2. 處理依據第一項被限制時，該個人資料，除儲存外，應僅限基於資料主體之同意、或為建立、行使或防禦法律上請求、或為保護他人或法人之權利、或基於歐盟法或會員國法律所定重要公共利益之理由，始得處理。

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

3. 資料主體依第一項規定已限制處理者，控管者於取消處理限制前，應通知資料主體。

Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

第十九條　關於更正或刪除個人資料或限制處理之通知義務

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

除經證明不可能為通知，或通知須花費過鉅之勞費者外，控管者應就第 16 條、第 17 條第 1 項及第 18 條所定之任何更正或刪除個人資料或限制處理向個人資料受揭露之各接收者為通知。控管者應依資料主體之要求向資料主體告知接收者。

Article 20 Right to data portability

第二十條　資料可攜性權利

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in

a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

1. 資料主體應有權以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並有權將之傳輸給其他控管者，而不受其提供個人資料之控管者之妨礙，如：
   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
   (a) 處理係基於第 6 條第 1 項第 a 點或第 9 條第 2 項第 a 點之同意或係基於第 6 條第 1 項第 b 點契約所為之者；及
   (b) the processing is carried out by automated means.
   (b) 處理係以自動化方式為之者。
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
2. 依據第一項行使其資料可攜性之權利者，如技術許可時，資料主體應有權使該個人資料由一控管者直接傳輸予其他控管者。
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
3. 本條第一項所定權利之行使不得優先於第 17 條規定。該權利於符合公共利益執行職務或委託資料控管者行使公權力而有必要為之處理者，不適用之。
4. The right referred to in paragraph 1 shall not adversely affect the rights

and freedoms of others.

4. 第一項所定權利不得影響他人之權利與自由。

Section 4 Right to object and automated individual decision-making

第四節　拒絕權及個人化之自動決策

Article 21 Right to object

第二十一條　拒絕權

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

1. 資料主體應有權基於與其具體情況有關之理由，隨時拒絕依第 6 條第 1 項第 e 點或第 f 點規定所為有關其個人資料之處理，包括基於該等條款所為之建檔。控管者應不得再處理該個人資料，除非該控管者證明其處理有優先於資料主體權利及自由之法律依據、或為建立、行使或防禦法律上請求所為之者。

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

2. 為直接行銷目的處理個人資料時，該資料主體有權隨時拒絕為行銷目的所涉及其個人資料之處理，包括與該直接行銷有關範圍內

之建檔。

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

3. 當資料主體拒絕為直接行銷目的而處理個人資料時，該個人資料不得再基於該目的而為處理。

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

4. 最遲於與資料主體第一次溝通時，應明確提請資料主體注意第 1 項及第 2 項所定權利，且清楚表達並與其他訊息區別。

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

5. 在使用資訊社會服務之過程中，不問第 2002/58/EC 號指令規範為何，資料主體得行使其權利，拒絕使用技術規範之自動化方式。

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

6. 如個人資料之處理係依據第 89 條第 1 項規定為科學或歷史研究目的或統計目的所為者，資料主體應有權基於與其具體情況有關之理由，拒絕與其有關之個人資料之處理，除非該處理係基於符合公共利益之職務執行之理由而有必要者。

Article 22 Automated individual decision-making, including profiling

第二十二條　個人化之自動決策，包括建檔

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

1. 資料主體應有權不受僅基於自動化處理（包括建檔）所做成而對其產生法律效果或類似之重大影響之決策所拘束。

2. Paragraph 1 shall not apply if the decision:

2. 第一項規定不予適用，如該決策：

   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   (a) 係為締結或履行資料主體與控管者間之契約所必要者；

   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (b) 係控管者受拘束之歐盟法或會員國法有明文授權，且定有適當之保護措施以確保資料主體之權利及自由及正當利益者；或

   (c) is based on the data subject's explicit consent.

   (c) 係基於資料主體之明確同意者。

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

3. 在第 2 項所定第 a 點及第 c 點之情形，資料控管者應執行適當保護措施以確保資料主體之權利及自由及正當利益，至少有權對控

管者部分為人為參與、表達意見以及挑戰該決策。

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4. 除第 9 條第 2 項第 a 點或第 g 點所定情形外，第 2 項所定決策不得係基於第 9 條第 1 項所定之特殊類型之個人資料，且應實施適當保護措施以確保資料主體之權利及自由及正當利益。

Section 5 Restrictions

第五節　限制

Article 23 Restrictions

第二十三條　限制

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

1. 資料控管者或處理者受拘束之歐盟法或會員國法得以立法程序限制第 12 條至第 22 條及第 34 條以及第 5 條所定之權利與義務之範圍，但限於其立法符合第 12 條至第 22 條所定之權利與義務，且該限制尊重基本權及自由之本質，並於民主社會中係必要且適當措施以確保：

   (a) national security;

   (a) 國家安全；

(b) defence;

(b) 防禦；

(c) public security;

(c) 公共安全；

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(d) 預防、調查、偵查及追訴刑事犯罪或執行刑罰，包括為維護及預防對公共安全造成威脅者；

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(e) 歐盟或會員國之一般公共利益的其他重要宗旨，尤其是歐盟或會員國之重要經濟或金融利益，包括財政、預算及稅負、公共衛生及社會安全；

(f) the protection of judicial independence and judicial proceedings;

(f) 司法獨立性及司法程序之保障；

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(g) 預防、調查、偵查及追訴違反特定職業之道德規範；

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(h) 依第 a 至 e 點及第 g 點所定情事，公務機關行使其監督、檢查或監管功能，即使係不定期性者；

(i) the protection of the data subject or the rights and freedoms of others;

(i) 保護資料主體或他人之權利及自由之保障；

(j) the enforcement of civil law claims.

(j) 民事請求之執行。

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

2. 尤其是，第 1 項所定之任何合法措施於相關情況下，應至少包含下列各款具體規定：

(a) the purposes of the processing or categories of processing;

(a) 處理之目的或處理之類型；

(b) the categories of personal data;

(b) 個人資料之類別；

(c) the scope of the restrictions introduced;

(c) 採用限制之範圍；

(d) the safeguards to prevent abuse or unlawful access or transfer;

(d) 防止濫用或非法接近使用或移轉之保護措施；

(e) the specification of the controller or categories of controllers;

(e) 控管者之標準或控管者之類型；

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(f) 儲存期間及考量到處理本質、範圍及目的之適當保護措施或處理類型；

(g) the risks to the rights and freedoms of data subjects; and

(g) 資料主體權利及自由之風險；及

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

(h) 資料主體關於該限制之知悉權，但限制之目的得優先於該權利者除外。

CHAPTER IV Controller and processor
第四章　控管者及處理者

Section 1 General obligations
第一節　一般義務

Article 24 Responsibility of the controller
第二十四條　控管者之責任

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

1. 考量到處理之性質、範圍、內容及目的以及當事人之權利及自由所受之諸多可能且嚴重之風險，控管者應實施適當科技化且有組織的措施以確保並得證明其處理符合本規則規定。該等措施應得予審視，且必要時應予更新。

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

2. 與處理活動相適當之情況下，第 1 項所定措施應包括控管者適當資料保護政策之實施。

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the

obligations of the controller.

3. 遵守第 40 條所定經批准之行為守則或第 42 條所定經核准之認證機制得作為控管者遵守其義務之證明。

Article 25 Data protection by design and by default

第二十五條　設計及預設之資料保護

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

1. 考量到現有技術、執行成本以及處理之性質、範圍、內容及目的以及處理對當事人之權利及自由所生諸多可能且嚴重之風險，不問係在決定處理方式時或係在處理中，控管者均應實施適當之科技化且有組織的措施，例如假名化，且該等措施旨在實現資料保護原則，如資料最少蒐集原則，並採取有效方式且將必要保護措施納入處理程序，以符合本規則之要求並保護資料主體之權利。

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's

intervention to an indefinite number of natural persons.

2. 控管者應實施適當之科技化且有組織的措施，以確保在預設情況下，僅處理一特定目的且必要限度範圍內之個人資料。該義務適用於所蒐集之個人資料之數量、處理之程度、儲存之期間及其可接近使用性。尤其是，該等措施於預設情況下，應確保個人資料不能經由人為干預而遭不特定人之接近使用。

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

3. 第 42 條所定經核准之認證機制得用以證明符合本條第 1 項及第 2 項所定之要求。

Article 26 Joint controllers

第 *26* 條　共同控管者

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

1. 兩個或兩個以上控管者共同決定處理之目的及方式時，其應為共同控管者。共同控管者應以透明之方式，彼此間安排，確定其各自履行本規則所定義務之責任，尤其是關於資料主體行使其權利及其各自對於第 13 條及第 14 條所定提供資訊所負之責任，但控管者受拘束之歐盟法或會員國法已就控管者各自之責任定有明文者不在此限。該安排得指定資料主體之聯絡對口。

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.
2. 第 1 項所定安排應適當反映共同控管者對於資料主體各自之任務及關係。該安排之重點應提供予資料主體。
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.
3. 不問第一項所定安排之條款為何，資料主體得依據本規則對任一控管者行使其權利。

Article 27 Representatives of controllers or processors not established in the Union

第二十七條　非設立於歐盟境內控管者或處理者之代表

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
1. 於第 3 條第 2 項有適用時，控管者或處理者應以書面指定歐盟境內之代表。
2. The obligation laid down in paragraph 1 of this Article shall not apply to:
2. 本條第 1 項所定義務，於下列情形不適用之：
   (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
   (a) 偶然性之處理，不包括大規模處理第 9 條第 1 項所定之特殊

類型個人資料或處理依第 10 條所定關於前科或犯罪之個人資料，且考量到處理之本質、過程、範圍與目的，不會對當事人之權利與自由造成風險者；或

(b) a public authority or body.

(b) 公務機關或機構。

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

3. 當處理活動涉及對資料主體提供貨品或服務或監控其行為者，代表應設立於資料主體所在之一會員國境內。

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

4. 除該控管者或處理者外，代表應由控管者或處理者授權涉及處理之所有問題，尤其係對於監管機關及資料主體，以確保遵守本規則之目的。

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

5. 控管者或處理者所指定之代表不得影響得對於控管者或處理者本身提起之法律行動。

Article 28 Processor

第二十八條　處理者

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a

manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

1. 處理係由控管者之代表所為者，控管者應僅得任用提供充足保證會實施適當之科技化且有組織的措施、使處理符合本規則要求、並確保資料主體權利保障之處理者。

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

2. 未經控管者事先個案或一般書面授權者，處理者不得與其它處理者相交涉。在一般書面授權情況下，處理者應通知控管者關於增加或替換其他處理者之任何預期變化，從而給予控管者對該等變化提出異議之機會。

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

3. 處理者所為處理應受契約或歐盟法或會員國法之其他立法之拘束，該等規定對於處理者及控管者具有拘束力，並規定處理標的及處理期間、處理之本質與目的、個人資料之類型及資料主體之類別以及控管者之義務及權利。該契約或其他立法尤其應規定處理者：

   (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required

to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(a) 僅得依據控管者之書面指示處理個人資料，包括移轉個人資料至第三國或國際組織，但處理者受拘束之歐盟法或會員國法要求其應為者不在此限；於此情形，除法律基於公共利益之重要理由禁止提供資訊者外，處理者於處理前應通知控管者該法定要求；

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(b) 確保被授權處理個人資料之人已承諾保密或具備適當之法定保密義務；

(c) takes all measures required pursuant to Article 32;

(c) 依第 32 條規定採取所有必要之保護措施；

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(d) 遵守第 2 項及第 4 項所定任用其它處理者之要件；

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(e) 考量到處理之本質，以適當之科技化且有組織的措施，在可能之情況下，協助控管者履行其回應資料主體行使第三章所定權利之請求之義務；

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(f) 考量到處理之本質及處理者可知資訊，協助控管者確保遵守第 32 條至第 36 條所定之義務；

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(g) 在提供與處理有關之服務結束後，依控管者之選擇，向控管者刪除或移轉所有個人資料，並刪除現有副本，但歐盟法或會員國法要求儲存該等個人資料者，不在此限；

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

(h) 向控管者提供證明遵守本條所定義務所需之一切資訊，並允許及促進由控管者或控管者委任之其他審計師進行查核，包括檢查。

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

關於第一款第 h 點，如處理者認為某指令是否違反本規則或其他歐盟或會員國資料保護規定者，應立即通知控管者。

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical

and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

4. 當處理者代表控管者與他處理者聯合進行特定之處理活動時，第 3 項所定控管者與處理者間之契約或其他立法規定之相同資料保護義務，應透過契約或歐盟法或會員國法所定之其他立法，使他處理者亦有其適用，尤其是提供充分保證其將實施適當之科技化且有組織的措施，使其處理符合本規則之要求。如他處理者未能履行其資料保護義務，則原處理者應就他處理者義務之履行對控管者負完全責任。

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

5. 處理者遵守第 40 條所定經核准之行為守則或第 42 條所定經核准之認證機制者，得作為本條第 1 項及第 4 項所定充分保證之證明。

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

6. 於無損及控管者及處理者間個別性契約之情況下，本條第 3 項及第 4 項所定契約或其他立法得全部或一部基於第 7 項及第 8 項所定之定型化契約條款，包括當其係依據第 42 條及第 43 條所定授予控管者或處理者認證之一部分時。

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in

accordance with the examination procedure referred to in Article 93(2).

7. 執委會得就本條第 3 項及第 4 項所定事項擬定定型化契約條款，並遵守第 93 條第 2 項所定之檢驗程序。

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

8. 監管機關得就本條第 3 項及第 4 項所定事項採用定型化契約條款，並遵守第 63 條所定之一致性機制。

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

9. 第 3 項及第 4 項所定契約或其他立法應以書面為之，包括電子形式。

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

10. 於無損及第 82 條、第 83 條及第 84 條規定之情況下，如處理者決定處理之目的與方式違反本規則者，該處理者應被視為係該處理之控管者。

Article 29 Processing under the authority of the controller or processor

第二十九條　控管者或處理者之處理權限

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

除歐盟法或會員國法另有規定外，處理者及基於控管者或處理者權限而接近使用個人資料之任何行為人，非基於控管者之指示者，不得處

理該等個人資料。

Article 30 Records of processing activities

第三十條　處理活動之紀錄

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

1. 任一控管者及控管者代表（如適用）應維護其負責之處理活動紀錄。該紀錄應包含下列所有資訊：

   (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

   (a) 控管者以及共同控管者（如適用）、控管者代表及資料保護員之名稱及聯絡方式；

   (b) the purposes of the processing;

   (b) 處理目的；

   (c) a description of the categories of data subjects and of the categories of personal data;

   (c) 資料主體類型及個人資料類別之描述；

   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

   (d) 個人資料已對其或將對其揭露之接收者類型，包括第三國或國際組織之接收者；

   (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

   (e) 將個人資料移轉至第三國或國際組織（如適用），包括指明

該第三國或國際組織，且若係第 49 條第 1 項第 2 款所定之移轉者，適當保護措施之書面文件；

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(f) 刪除不同類別之個人資料之預設時間上限（如可能）；

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(g) 第 32 條第 1 項所定科技化且有組織之安全措施之概述（如可能）；

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

2. 各處理者及處理者代表（如適用）應維護代表控管者所進行之所有類別處理活動之紀錄，包括：

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(a) 各控管者及代各控管者進行處理之一個或多個處理者及該各控管者或處理者代表（如適用）及資料保護員之名稱及聯絡方式；

(b) the categories of processing carried out on behalf of each controller;

(b) 各控管者之代表所進行之處理類型；

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(c) 將個人資料移轉至第三國或國際組織（如適用），包括指明

該第三國或國際組織，且若係第 49 條第 1 項第 2 款所定之移轉者，適當保護措施之書面文件；

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(d) 第 32 條第 1 項所定科技化且有組織之安全措施之概述（如可能）；

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

3. 第 1 項及第 2 項所定紀錄應以書面為之，包括電子形式。

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

4. 控管者或處理者及控管者或處理者代表 (如適用) 應依監管機關之要求提供紀錄。

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

5. 第 1 項及第 2 項所定義務不適用於員工人數低於 250 人以下之企業或組織，除非其所為之處理會造成資料主體權利及自由之風險、非偶然性之處理、或其處理包括第 9 條第 1 項所定特殊類型之個人資料、或為第 10 條所定涉及前科及犯罪之個人資料。

Article 31 Cooperation with the supervisory authority

第三十一條　與監管機關之合作

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the

performance of its tasks.
控管者及處理者應依要求與監管機關合作執行其職務。控管者及處理者之代理人於得適用時，亦同。

Section 2 Security of personal data
第二節　個人資料之安全

Article 32 Security of processing
第三十二條　處理之安全

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. 考量現有技術、執行成本、處理之本質、範圍、脈絡及目的與對當事人權利及自由之風險變動之可能性與嚴重性，控管者及處理者應執行採取適當之科技化且有組織的措施，以確保對於風險之適當安全程度，包括但不限於適當之如下事項：

   (a) the pseudonymisation and encryption of personal data;
   (a) 個人資料之假名化及加密；
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   (b) 確保處理系統及服務持續之機密性、完整性、可用性及彈性之能力；
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (c) 在物理性或技術性事件中及時回復個人資料可用性及可接近

性之能力；

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(d) 定期測試，評估並衡量確保處理安全性之科技化且有組織之措施之有效性。

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. 於衡量適當之安全程度時，尤其應考量因處理而造成之風險，特別是來自意外或非法破壞、損失、改變、未獲授權之揭露、或經傳輸、儲存或其他處理之個人資料之接近權。

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

3. 恪守第 40 條所稱經核准之行為守則或第 42 條所稱經核准之認證機制，得作為顯示遵循本條第 1 項要求之斟酌因素之一。

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

4. 控管者及處理者應採取行動，確保任何受該取得個人資料之控管者或處理者指揮之個人不得為指示外之處理，但其受歐盟法或會員國法要求而為之者，不在此限。

Article 33 Notification of a personal data breach to the supervisory authority

第三十三條　向監管機關進行個人資料侵害之通報

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1. 於個人資料侵害發生時，控管者即應依第 55 條向監管機關通報，不得無故遲延，且如可能，應於發現後 72 小時內通報，但個人資料侵害無造成對當事人權利及自由之風險時，不在此限。於未於 72 小時內向監管機關通報之情形，通報應附遲延之理由。

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

2. 發現個人資料侵害後，處理者應通報控管者，不得無故遲延。

3. The notification referred to in paragraph 1 shall at least:

3. 第 1 項之通報至少應：

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(a) 描述個人資料侵害之本質，如有可能，應包括相關資料主體之類型及大致數量，及相關個人資料紀錄之類型及大致數量；

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(b) 告知資料保護員之姓名及聯絡細節，或其他得獲得更多資訊

之聯絡者；

(c) describe the likely consequences of the personal data breach;

(c) 描述個人資料侵害之可能結果；

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(d) 描述控管者已採取或預計採取用以處理個人資料侵害之措施，如適當，應包括降低可能不利影響之措施。

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4. 於目前無法同時提供資訊時，資訊應分階段提供，不得有進一步之無故遲延。

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

5. 控管者應記載任何個人資料侵害，包括與個人資料侵害相關之事實、其影響及已採取之救濟措施。該等記載應得由監管機關查驗是否與本條相符。

Article 34 Communication of a personal data breach to the data subject

第三十四條　向資料主體為個人資料侵害之溝通

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

1. 於個人資料侵害可能導致當事人權利及自由之高風險時，控管者應與資料主體溝通個人資料侵害，不得無故遲延。

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

2. 本條第 1 項所稱向資料主體之溝通，應以清楚簡易之語言描述個人資料侵害，並至少包括第 33 條第 3 項第 (b)、(c)、及 (d) 點之資訊及措施。

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

3. 第 1 項所稱向資料主體之溝通，遇有符合下列條件之一者，應無須被要求為之：

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(a) 控管者已執行適當之科技化與有組織之措施，且該等措施已適用於受個人資料侵害影響之個人資料，尤其已使未獲授權接近使用之人無法識別個人資料者，如加密；

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(b) 控管者已採取後續措施，確保第 1 項所稱對資料主體權利及自由之高風險已不會實現；

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(c) 涉及不符比例之努力。於此情形，應有公共溝通或類似措施取代之，使資料主體獲相同有效之通知。

4. If the controller has not already communicated the personal data breach

to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

4. 於控管者尚未向資料主體溝通個人資料侵害時，監管機關得考量個人資料侵害可能導致高風險，要求控管者進行溝通或認定第 3 項之任一條件已符合。

Section 3 Data protection impact assessment and prior consultation

第三節　資料保護影響評估與事前諮詢

Article 35 Data protection impact assessment

第三十五條　資料保護影響評估

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

1. 於特別使用新科技之處理方式，且考量該處理之本質、範圍、使用情形及目的後，認為該處理可能導致自然人之權利及自由的高度風險時，控管者應於處理前，實行該處理對於個人資料保護之影響評估。單一評估得針對一系列呈現相似高風險之類似處理。

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

2. 實行資料保護影響評估時，控管者應尋求資料保護員之意見。

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

3. 第 1 項所稱資料保護影響評估於下列情形應特別被要求：

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(a) 關於自然人之系統性及大規模的個人特質評估，而該評估是基於自動處理，包含建檔，且基於該評估作成關於該自然人之法律效果或其他重大影響該自然人之決定；

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(b) 處理大規模之第 9 條第 1 項所稱之特殊類型個人資料，或關於第 10 條所稱前科及犯罪之個人資料；

(c) a systematic monitoring of a publicly accessible area on a large scale.

(c) 大規模系統性監督公共區域。

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.
The supervisory authority shall communicate those lists to the Board referred to in Article 68.

4. 監管機關應建立並公布依第 1 項需要資料保護影響評估之處理類型清單。監管機關應與第 68 條所稱之委員會溝通該清單。

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

5. 監管機關亦得建立並公布不需要資料保護影響評估之處理類型清單。監管機關應與委員會溝通該清單。

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

6. 於採用第 4 項及第 5 項所稱之清單前，於該等清單涉及有關提供商品或服務與資料主體或有關在各會員國監督其行為，或可能實質影響個人資料於歐盟自由流通等之處理活動時，主管監管機關應適用第 63 條所稱之一致性機制。

7. The assessment shall contain at least:

7. 評估應至少包含：

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(a) 擬採用處理之系統性描述及該處理之目的，於可適用之情形，包含控管者追求之合法利益；

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(b) 該處理之必要性及比例性與目的間之關係評估；

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(c) 對於第 1 項所稱資料主體之權利及自由之風險評估；及

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data

subjects and other persons concerned.

(d) 應對風險之方式，包含保護措施、保全措施及確保個人資料保護及符合本規則考慮資料主體及其他相關人員之權利及合法利益之機制。

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

8. 第 40 條所稱經核准之行為守則是否為相關控管者或處理者所遵循，應於評估由該等控管者或處理者所為之處理所造成之影響時，予以慎重考慮，特別是為資料保護影響評估之目的時。

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

9. 在不實質影響商業或公共利益之保護或處理之保全的前提下，於適當時，控管者應尋求資料主體或其代表人對於處理之意見。

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

10. 於依第 6 條第 1 項第 c 點或第 e 點之處理有控管者遵循之歐盟法或會員國法之法律基礎，而該法管制特定處理或有爭議之處理，且資料保護影響評估已因採用該法律基礎而於概括影響評估中實行時，除會員國認為有必要於處理活動前實行該評估外，第 1 項

至第 7 項不適用之。

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

11. 於必要時，控管者至少應於處理之風險有變化時，審查評估是否依資料保護影響評估實行處理。

Article 36 Prior consultation

第三十六條　事前諮詢

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

1. 當資料保護影響評估依第 35 條顯現若控管者未採取降低風險之措施，該處理將導致高風險時，控管者應於處理前諮詢監管機關。

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

2. 當監管機關認為第 1 項所稱之處理將違反本規則，尤其是當控管

者未能完全指出或減低風險時，監管機關應於收受諮詢請求後 8 周內，提供書面意見予控管者並視情形予處理者，並得行使其於第 58 條所載之任何權力。該期間可因處理之複雜程度再延長 6 周。監管機關應於收受諮詢請求後 1 個月內通知控管者並視情形通知處理者上開延期情況及延期原因。該等期間得中止至監管機關取得提供諮詢所需之資訊。

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

3. 依第 1 項諮詢監管機關時，控管者應提供監管機關：

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(a) 於可適用時，涉及處理之控管者、共同控管者及處理者分別之責任，尤其是在企業集團內所為之處理；

(b) the purposes and means of the intended processing;

(b) 該處理之目的及方法；

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(c) 依本規則保護資料主體權利及自由之措施及保護方式；

(d) where applicable, the contact details of the data protection officer;

(d) 於可適用時，資料保護員之詳細聯絡方式；

(e) the data protection impact assessment provided for in Article 35; and

(e) 依第 35 條提供之資料保護影響評估；及

(f) any other information requested by the supervisory authority.

(f) 其他任何監管機關要求之資訊。

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

4. 會員國應於提出將由國會採納之立法措施建議之準備期間，或依該立法措施之管制措施的準備期間，視何者與處理有關，而諮詢監管機關。

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

5. 會員國法得不受第 1 項之拘束，要求控管者針對由控管者為公共利益履行任務之處理，包含與社會保護及公共健康有關之處理，諮詢並自監管機關取得事前授權。

Section 4 Data protection officer
第四節　資料保護員

Article 37 Designation of the data protection officer
第三十七條　資料保護員之指定

1. The controller and the processor shall designate a data protection officer in any case where:

1. 於下列任一情形，控管者及處理者應指定資料保護員：

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(a) 除法院行使其司法權外，該處理係由公務機關或機構執行；

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(b) 控管者或處理者之核心活動，包括依其本質、範圍及 / 或其

目的，需要定期且系統性地大規模監控資料主體；或

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

(c) 控管者或處理者之核心活動，包括第 9 條所稱之大規模處理特殊類型之資料及第 10 條所稱之前科與犯罪相關之個人資料。

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

2. 於各分支機構皆易於接近單一一名資料保護員時，企業集團得指定同一名資料保護員。

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

3. 於控管者或處理者為公務機關或機構時，考量其組織結構與規模，單一一名資料保護員得受指定至多個該等機關或機構。

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

4. 於第 1 項以外之情形，控管者、處理者或組織及其他代表控管者或處理者類型之機構得指定資料保護員，或於歐盟或會員國法要求時應指定之。

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data

protection law and practices and the ability to fulfil the tasks referred to in Article 39.

5. 資料保護員應依專業資格、尤其資料保護法律與實踐之專業知識、及完成第 39 條所稱職務之能力指定之。

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

6. 資料保護員得為控管者或處理者之工作人員，或基於服務契約完成職務。

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

7. 控管者或處理者應公告資料保護員之契約細節，並向監管機關溝通之。

Article 38 Position of the data protection officer
第三十八條　資料保護員之職位

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

1. 控管者及處理者應確保資料保護員適當且及時涉入所有有關個人資料保護之業務。

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

2. 控管者及處理者應透過提供為執行職務及對個人資料與處理活動之可及性所必要、以及維持其專業知識所必要之資源，支持資料保護員行使第 39 條所稱職務。

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those

tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

3. 控管者及處理者應確保資料保護員免於接收任何有關執行職務之指令。其不得因執行職務而被控管者或處理者解任或處罰。資料保護員應直接向處理者或管理者之最高管理階層報告。

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

4. 資料主體就所有與其個人資料處理及行使本規則權利之有關原因，得聯繫資料保護員。

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

5. 資料保護員應依歐盟或會員國法，就其職務負保密義務。

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

6. 資料保護員得完成其他職務與職責。控管者或處理者應確保任何該等職務與職責不致利害衝突。

Article 39 Tasks of the data protection officer

第三十九條　資料保護員之職務

1. The data protection officer shall have at least the following tasks:

1. 資料保護員應至少有下列之職務：

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(a) 依本規則及其他歐盟或會員國法之資料保護規定通知並建議控管者或處理者及執行其義務之員工；

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(b) 監督本規則、其他歐盟或會員國法之資料保護規定及與個人資料保護相關對控管者或處理者之政策，包括責任分配、提高認識及工作人員關於處理活動之訓練、以及相關審計之遵循；

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(c) 於受資料保護影響評估請求時，提供建議，並依第 35 條監督其執行；

(d) to cooperate with the supervisory authority;

(d) 與監管機關合作；

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

(e) 於處理相關之議題，包括第 36 條所稱之事前諮詢時，擔任監管機關之連絡站，並於適當時提供其他事項之諮詢；

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2. 資料保護員於執行其職務時，應考量處理之本質、範圍、脈絡及

目的，適當考慮處理活動所涉風險，

Section 5 Codes of conduct and certification
第五節　行為守則與認證

Article 40 Codes of conduct
第四十條　行為守則

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
1. 會員國、監管機關、委員會及執委會對於行為守則之訂立，應給予鼓勵，以促進本規則之有效適用，並考量某些行業執行資料處理之特定特徵及微型、中小型企業之特定需求。
2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
2. 組織與代表控管者或處理者類型之其他機構得備置行為守則或修改或擴張該守則以明確化本規則之適用範圍，例如：
   (a) fair and transparent processing;
   (a) 公正及透明之處理；
   (b) the legitimate interests pursued by controllers in specific contexts;
   (b) 控管者於具體情況下追求之正當利益；
   (c) the collection of personal data;
   (c) 個人資料之蒐集；
   (d) the pseudonymisation of personal data;
   (d) 個人資料之假名化；

(e) the information provided to the public and to data subjects;

(e) 提供大眾及資料主體之資訊；

(f) the exercise of the rights of data subjects;

(f) 資料主體權利之行使；

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(g) 向兒童提供之資訊及對於兒童之保護，以及獲得其法定代理人同意之方式；

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(h) 第 24 條及第 25 條所定之方式及程序，及第 32 條所定確保處理安全性之保護措施；

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(i) 向監管機關通知個人資料之侵害，以及將該等個人資料侵害通知資料主體；

(j) the transfer of personal data to third countries or international organisations; or

(j) 個人資料移轉至第三國或國際組織；或

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

(k) 法庭外程序與其他爭端解決程序，用以解決控管者和資料主體間關於處理之爭議，而不損及第 77 條及第 79 條所定之資料主體之權利。

3. In addition to adherence by controllers or processors subject to this

Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

3. 本條第 5 項所定經核准及本條第 9 項所定具有一般規範效力之行為守則，除適用於受本規則拘束之控管者或處理者外，亦得適用於第 3 條所定不受本規則拘束之控管者或處理者，使其依第 46 條第 2 項第 e 點規定將個人資料移轉至第三國或國際組織時得以提供適當之保護措施。該等控管者或處理者應透過契約或其他具有法律拘束力之文書，做成具有拘束力且可得執行之承諾，以適用該等適當之保護措施，包括關於資料主體之權利。

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

4. 本條第 2 項所定之行為守則應涵蓋得以使第 41 條第 1 項所定機構對承諾遵守該等規範之控管者或處理者進行強制性監控之機制，而不損及第 55 條或 56 條所定主管監管機關之任務及權力。

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55.

The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

5. 本條第 2 項所定欲備置行為守則或修改或擴張現存行為守則之組織及其他機構，應將該行為守則草案、修正案或擴充案提交至第 55 條所定之主管監管機關。該監管機關應提供該草案、修正案或擴充案是否符合本規則之意見，如其認為已提供充分且適當之保護措施者，即應核准該草案、修正案或擴充案。

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

6. 依第 5 項規定核准行為守則草案或修正案或擴充案，且該行為守則與多個會員國之處理活動無關者，監管機關應登記並公布該行為守則。

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

7. 如行為守則涉及多個會員國之處理活動者，第 55 條所定之主管監管機關於核准該草案、修正案或擴充案前，應依照第 63 條所定程序將之提交至委員會，使其就該草案、修正案或擴充案是否符合本規則之規定或是否已依本條第 3 項規定提供適當保護乙節表示意見。

8. Where the opinion referred to in paragraph 7 confirms that the draft

code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

8. 第 7 項所定之意見確認該草案、修正案或擴充案符合本規則或已依照第 3 項規定提供適當保護者，委員會應將其意見提交至執委會。

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

9. 執委會得以施行法之方式，決定本條第 8 項所定經提交且核准之行為守則、修正案及擴充案於歐盟內具有一般規範效力。該等施行法應依照第 93 條第 2 項所定檢驗程序通過。

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

10. 執委會應確保依照第 9 項規定具有一般規範效力且經核准之行為守則之公示性。

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

11. 委員會應將所有經核准之行為守則、修正案及擴充案整理登錄，並應以適當方式公開之。

Article 41 Monitoring of approved codes of conduct
第四十一條　經核准之行為守則之監管

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body

which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

1. 在不損及第 57 條及 58 條所定主管監管機關之任務及權力之情況下，得由機構進行第 40 條所定對行為守則遵守情況之監測，該機構應具備行為守則所涉及事件之適當程度之專業知識，且經主管監管機關認證。

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

2. 第 1 項所定得經認證以監測行為守則被遵守情況之機構，應具備：

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(a) 證明其具備行為守則所涉及事件之獨立性及專業性至主管監管機關滿意；

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(b) 建立使其得以評估控管者及處理者適用該行為守則之資格之程序，以監測其遵守情況，並定期審查其運作情形；

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(c) 建立處理申訴之程序及組織，以處理違反行為守則或控管者或處理者執行之方式已違反或正違反行為守則之申訴，並向資料主體及公眾公開該等程序及組織；及

(d) demonstrated to the satisfaction of the competent supervisory

authority that its tasks and duties do not result in a conflict of interests.

(d) 證明其任務及責任不會產生利害衝突至主管監管機關滿意。

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

3. 主管監管機關應依照第 63 條所定一致性機制，向委員會提交本條第 1 項所定機構之認證標準草案。

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

4. 在不損及主管監管機關之任務及權力且第 8 章規定之情況，本條第 1 項所定機構應在適當保護措施下，對於控管者或處理者違反行為守則事件採取適當行動，包括將控管者或處理者停權或於行為守則中剝除。其對於控管者或處理者所為行為及其理由應通知主管監管機關。

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

5. 機構欠缺認證要件或不再具備認證要件或機構行為違反本規則規定者，主管監管機關應撤銷第一項所定之認證。

6. This Article shall not apply to processing carried out by public authorities and bodies.

6. 本條不適用於公務機關及機構之處理。

Article 42 Certification

第四十二條　認證

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

1. 會員國、監管機關、委員會及執委會應鼓勵，尤其係歐盟層級，建立資料保護認證機制與資料保護標章及標誌，以證明控管者及處理者之處理活動遵守本規則。微型及中小型企業之具體需求應予考慮。

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

2. 本條第 5 項所定經核准之資料保護認證機制與資料保護標章及標誌，除適用於受本規則拘束之控管者或處理者外，亦得為第 3 條所定不受本規則拘束之控管者或處理者依第 46 條第 2 項第 f 點規定將個人資料移轉至第三國或國際組織時，用以證明適當保護措施之存在。該等控管者或處理者應透過契約或其他具有法律拘束

力之文書，做成具有拘束力且可得執行之承諾，以適用該等適當之保護措施，包括關於資料主體之權利。

3. The certification shall be voluntary and available via a process that is transparent.

3. 認證應係志願性的，並透過透明程序取得。

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

4. 本條所定認證不減損控管者或處理者遵守本規則之責任，且不損及第 55 條或第 56 條所定主管監管機關之任務及權力。

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

5. 本條所定之認證應由認證機構依第 43 條規定或主管監管機關依據第 58 條第 3 項所核准之標準或由委員會依第 63 條規定為之。委員會核准之標準得為通用性認證，即歐盟資料保護標章。

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

6. 將處理提交至認證機制之控管者或處理者應向第 43 條所定之認證機構或主管監管機關（如適用）提供認證程序所需關於其處理活動之所有資訊及接近使用之方式。

7. Certification shall be issued to a controller or processor for a maximum

period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

7. 對控管者或處理者所為之認證，最長期限應為三年，且在相同要件下並持續符合相關要求者，得更新之。第 43 條所定之認證機構或主管監管機關（如適用）於欠缺認證要件或不再符合認證要件之情況下，應撤回認證。

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

8. 委員會應將所有資料保護認證機制與資料保護標章及標誌整理登錄，並應以適當方式公開之。

Article 43 Certification bodies

第四十三條　認證機構

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

1. 在不損及第 57 條及 58 條所定主管監管機關之任務及權力之情況下，具備關於資料保護之適當程度專業性之認證機構，於通知監管機關使其得於必要時依照第 58 條第 2 項第 h 點行使其權力後，核發及更新認證。會員國應確保該等認證機構通過下列一項或二項之認證：

   (a) the supervisory authority which is competent pursuant to Article

55 or 56;

(a) 第 55 條或第 56 條所定之主管監管機構；

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[2] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

(b) 依 EN-ISO/IEC 第 17065/2012 號標準以及主管監管機關依第 55 條或第 56 條規定所建立之附加要求，按歐洲議會及歐盟理事會 [2] 第 765/2008 號規則命名之國家認證機構。

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

2. 第 1 項所定之認證機構應依該項規定通過認證，但必須符合以下要件：

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(a) 證明其具備所涉及認證事件之獨立性及專業性至主管監管機關滿意；

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(b) 承諾會遵守第 42 條第 5 項所定之標準，並經主管監管機關依

[2] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).
歐洲議會及歐盟理事會 2008 年 7 月 9 日第 765/2008 規則制定關於產品銷售認證及市場監管之要求，並廢止第 339/93 號歐盟規則（官方公報 L 類，2008 年 8 月 13 日，第 30 頁）。

第 55 條或第 56 條規定、或經委員會依第 63 條規定核准；

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(c) 建立資料保護認證、資料保護標章及標誌的核准、定期審查及撤回之程序；

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) 建立處理申訴之程序及組織，以處理違反資料保護認證或控管者或處理者執行之方式已違反或正違反資料保護認證之申訴，並向資料主體及公眾公開該等程序及組織；及

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

(e) 證明其任務及責任不會產生利害衝突至主管監管機關滿意。

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

3. 本條第 1 項及第 2 項所定認證機構之認證應由主管監管機關依據第 55 條或第 56 條規定或由委員會依第 63 條規定依其核准之標準定之。依據本條第 1 項第 b 點之認證，該等要件應與第 765/2008 號規則及規範認證機構之方法及程序之技術規則相一致。

4. The certification bodies referred to in paragraph 1 shall be responsible

for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

4. 第 1 項所定之認證機構應負責對於認證及撤回認證進行適當之評估，但不損及控管者或處理者遵守本規則之責任。認證最長期限為 5 年，且得在相同要件下更新，但該認證機構應符合本條所定之要求。

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

5. 第一項所定之認證機構應向主管監管機關提供核准或撤回認證之理由。

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

6. 本條第 3 項所定要件及第 42 條第 5 項所定標準應由監管機關以方便取得之格式公開之。監管機關亦應將該等要件及標準傳送至委員會。委員會應將所有資料保護認證機制與資料保護標章整理登錄，並應以適當方式公開之。

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where

actions taken by a certification body infringe this Regulation.

7. 在不損及第 8 章規定之情況下，主管監管機關或國家認證機構於欠缺認證要件或不再符合認證要件或認證機構之行為違反本規則之情況下，應依本條第 1 項規定撤銷該認證機構之認證。

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

8. 執委會應有權依據第 92 條規定通過授權法，以具體化第 42 條第 1 項所定資料保護認證機制應考慮的要件。

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

9. 執委會得通過施行法，為資料保護認證機制與資料保護標章及標誌制定技術性標準，以促進及認可該等資料保護認證機制與資料保護標章及標誌。該等施行法應依照第 93 條第 2 項所定之檢驗程序通過。

CHAPTER V Transfers of personal data to third countries or international organisations

第五章　個人資料移轉至第三國或國際組織

Article 44 General principle for transfers

第四十四條　移轉之一般原則

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.
任何經處理或於移轉至第三國或國際組織後將欲處理之個人資料之移轉，僅得於控管者及處理者遵循本章之條件下進行，並符合本規則其他條文，包括從第三國或國際組織所為之進一步移轉。為確保本規則保證之當事人保護程度不受減損，本章所有條文應受適用。

Article 45 Transfers on the basis of an adequacy decision
第四十五條　基於充足程度保護決定之移轉

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
1. 個人資料移轉至第三國或國際組織，僅於執委會決定該第三國、第三國內之領域或特定部門、或國際組織確有充足程度之保護時，方得為之。該移轉不須獲得任何特別授權。
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
2. 於評估保護程度之充足性時，執委會尤其應考量下列因素：
   (a) the rule of law, respect for human rights and fundamental freedoms, 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, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(a) 法治、對人權與基本自由之尊重、一般與部門之相關立法，包括有關公共安全、防衛、國家安全及刑法、公務機關對個人資料之接近使用權、及該等立法、資料保護規則、專業規則及安全措施之執行，包括個人資料向其他第三國或國際組織進一步移轉，該其他第三國或國際組織之規則、判例法、及有效且可執行之資料主體權利及個人資料受移轉之資料主體有效之行政與司法救濟；

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(b) 第三國內有一個或以上獨立監管機關之存在及有效運作，或對象為國際組織時，確保及執行資料保護規則之遵守，包括充足之執行權，以協助及建議資料主體行使其權利，並與會員國之監管機關合作；及

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations

arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

(c) 第三國或國際組織所加入之國際協定，或其他因具法律拘束力之合約或辦法、及從其參與多邊或區域體系而生之義務，尤其關於個人資料保護者。

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

3. 執委會於評估保護之充足程度後，得透過施行法決定第三國、第三國內之領域或單一或多數之特定部門、或國際組織依本條第 2 項之方式確保充足程度保護。施行法應提供定期檢驗機制，至少四年一次，並應考量第三國或國際組織之所有相關發展。施行法應特定其適用之領域及部門，且於得適用時，確認監管機關或本條第 2 項第 b 點所稱之機關。施行法應採行第 93 條第 2 項之檢驗程序。

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/

EC.

4. 執委會應持續監控如下之第三國與國際組織，亦即：可能影響依本條第 3 項採行之決定、及依歐盟指令第 95/46/EC 號第 25 條第 6 項採行之決定運作之發展。

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

5. 於現有資訊顯示，尤其依本條第 3 項之檢驗，第三國、第三國內之領域或單一或多數之特定部門、或國際組織不再確保本條第 2 項意義下之充足程度保護時，執委會應於必要程度內透過執行不具溯及既往效力之行為，廢除、修正或凍結本條第 3 項。該等施行法應依第 93 條第 2 項之檢驗程序行之。於具正當理由之緊急情形，執委會應依第 93 條第 3 項之程序立即採用可適用之施行法。

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

6. 執委會應參與與第三國或國際組織之協商，以救濟依第 5 項作成決定之情形。

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international

organisation in question pursuant to Articles 46 to 49.

7. 本條第 5 項之決定不損及第 46 條至第 49 條所指向第三國、第三國內之領域及特定部門、及國際組織之個人資料移轉。

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

8. 執委會應於歐洲聯盟官方公報及網站上，公布已決定或不再確保具充足程度保護之第三國、第三國內之領域及特定部門、及國際組織之名單。

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

9. 執委會基於歐盟指令第 95/46/EC 號第 25 條第 6 項採行之決定，於執委會依本條第 3 項或第 5 項決定修改、取代或廢除前，應持續有效。

Article 46 Transfers subject to appropriate safeguards
第四十六條　須遵守適當保護措施之移轉

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

1. 於欠缺第 45 條第 3 項之決定時，控管者或處理者僅於其提供適當保護措施，且資料主體之權利得為執行，並具備有效權利救濟時，始得移轉個人資料至第三國或國際組織。

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

2. 第 1 項所稱之適當保護措施，於無監管機關為特定授權之情形下，得以下列方式提供：

(a) a legally binding and enforceable instrument between public authorities or bodies;

(a) 與公務機關或機構間有法律拘束力且得執行之辦法；

(b) binding corporate rules in accordance with Article 47;

(b) 第 47 條之有拘束力之企業守則；

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(c) 執委會依第 93 條第 2 項之檢驗程序採行之標準資料保護條款；

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(d) 監管機關採行，並由執委會依第 93 條第 2 項之檢驗程序核准之標準資料保護條款；

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(e) 依第 40 條經核准之行為守則，及第三國之控管者或處理者有拘束力且可執行之協約，以適用適當保護措施，包括關於資料主體之權利；或

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

(f) 依第 42 條經核准之驗證機制，及第三國之控管者或處理者有拘束力且可執行之協約，以適用適當保護措施，包括關於資料主體之權利。

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

3. 第 1 項所稱之適當保護措施，於有主管監管機關為授權之情形下，得以下列方式提供：

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(a) 控管者或處理者與第三國或國際組織之個人資料控管者、處理者或接收者間之契約條款；

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(b) 納入包括可執行且有效之資料主體權利之公務機關或機構間行政安排之條款。

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

4. 於本條第 3 項之情形，監管機關應遵循第 63 條之一致性機制。

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

5. 會員國或監管機關依歐盟指令第 95/46/EC 號第 26 條第 2 項之授

權，於監管機關認有必要而修改、取代或廢除前，應持續有效。依歐盟指令第 95/46/EC 號第 26 條第 4 項之決定，於執委會認有必要而依本條第 2 項決定修改、取代或廢除前，應持續有效。

Article 47 Binding corporate rules

第四十七條　有拘束力之企業守則

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

1. 於有拘束力之企業守則符合下列條件時，主管監管機關應依第 63 條之一致性機制核准之：

   (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

   (a) 法律上拘束並由共同經濟活動中之各事業團體或企業團體之成員適用與遵守，包括其員工；

   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

   (b) 明文賦予資料主體關於其個人資料處理可執行之權利；及

   (c) fulfil the requirements laid down in paragraph 2.

   (c) 符合第 2 項之要求。

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

2. 第 1 項所稱有拘束力之企業守則至少應特定：

   (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

   (a) 共同經濟活動中之事業團體或企業團體及其各成員之組織與聯絡方式；

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(b) 資料移轉或一系列移轉，包括個人資料之類型、處理之類型及目的、受影響之資料主體類型、及該第三國之識別；

(c) their legally binding nature, both internally and externally;

(c) 其內部及外部具合法拘束力之本質；

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(d) 一般資料保護原則之適用，尤其目的限制、資料最少蒐集原則、資料品質、設計或預設資料保護、處理之法律依據、特殊類型個人資料之處理、確保資料安全之措施、及進一步移轉至不受具拘束力之企業守則所拘束之機構時之要求；

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(e) 資料主體關於處理之權利及行使該等權利之方式，包括不得僅受自動化處理決定之權利（含第 22 條之建檔）、依第 79 條向主管監管機關及會員國之管轄法院提起申訴、及如適合

時，因有拘束力之企業守則之侵害而獲得補償之權利；

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(f) 設立於會員國之控管者或處理者承受其歐盟境外之成員任何違反有拘束力之企業守則時之責任；控管者或處理者應僅於證明該成員對造成損害結果不負責任時，全部或部分免除責任；

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(g) 有拘束力之企業守則之資訊，尤其本項第 d、e 及 f 點所稱之規定，如何於第 13 條及第 14 條外提供予資料主體；

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(h) 依第 37 條受指定之任何資料保護員、或共同經濟活動中之事業團體或企業團體內，其他任何負責監控有拘束力之企業守則之遵守情形、及監督培訓及申訴處理之人或實體之職務；

(i) the complaint procedures;

(i) 申訴程序；

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the

verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(j) 共同經濟活動中之事業團體或企業團體確保有拘束力之企業守則遵循之驗證機制。該等機制應包括資料保護審計及確保糾正措施以保護資料主體權利之方法。該等驗證之結果應向第 h 點所稱之個人或實體及共同經濟活動中之事業團體或企業團體之控管階層溝通，並應於主管監管機關請求時提供；

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(k) 報告及紀錄規範之變更及向監管機關報告該等變更；

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(l) 與監管機關之合作機制，以確保任何共同經濟活動中之事業團體或企業團體之成員遵循，尤其是監管機關請求依第 j 點措施驗證之結果時，應予提供；

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(m) 於共同經濟活動中之事業團體或企業團體之成員可能涉及對有拘束力之企業守則所保證者有實質不利影響時，向主管監管機關報告任何法律要求之機制；

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

(n) 針對永久或定期接觸個人資料之人員之適當資料保護訓練。

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

3. 執委會得特定本條意義下有拘束力之企業守則關於控管者、處理者及監管機關間交換資訊之形式與程序。該等執行規範應符合第 93 條第 2 項設定之檢驗程序。

Article 48 Transfers or disclosures not authorised by Union law
第四十八條　未獲歐盟法授權之移轉或揭露

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

第三國任何法院或法庭裁判及任何行政機關決定，如有要求控管者或處理者移轉或揭露個人資料者，僅得在基於有效存在於請求之第三國及歐盟或會員國間之國際協約，如雙邊法律協助條約，且不損及本章所定移轉之其他法律依據時，始得獲承認或可得執行。

Article 49 Derogations for specific situations

第四十九條　特定情形下之例外

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

1. 於欠缺第 45 條第 3 項之充足程度保護之決定、或欠缺第 46 條之適當保護措施時，包括有拘束力之企業守則、個人資料之移轉或一系列移轉至第三國或國際組織，僅應於符合下列條件時進行：

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(a) 資料主體於受關於因欠缺充足程度保護決定及適當保護措施，該等移轉對資料主體造成之可能風險通知後，已明確同意計畫之移轉；

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(b) 移轉對履行資料主體與控管者間契約、或依資料主體之請求執行契約前之措施為必要；

(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 another natural or legal person;

(c) 移轉對締結或履行控管者與其他自然人或法人間，基於資料主體之利益所締結之契約為必要；

(d) the transfer is necessary for important reasons of public interest;

(d) 移轉對公共利益之重要原因為必要；

(e) the transfer is necessary for the establishment, exercise or defence

of legal claims;

(e) 移轉對建構、行使或防禦法律上之請求為必要；

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(f) 於資料主體身體上或法律上無法為同意之表示時，移轉對保護資料主體之重要利益為必要；

(g) the transfer is made from a register which according to Union or Member State law 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 a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

(g) 移轉係依據歐盟或會員國法登記，意圖提供公眾信息且開放予一般公眾或任何得舉證具合法利益者諮詢，但僅限於特定情形中歐盟或會員國法設定之諮詢條件獲滿足之程度。

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

於移轉無法符合第 45 條或第 46 條之規定，包括有拘束力之企業守則之規定，且無法適用本項第 1 款所稱之任何特定例外情形時，向第三國或國際組織之移轉僅於該移轉非重複性、僅影響有限數量之資料主體，對控管者所追求之合法目的為必要而不凌駕於資料主體之利益或權利及自由，且控管者已評估資料移轉之所有環境，而立於評估對個人資料保護為適合保護措施之基礎時，方得進行。控管者應將移轉通知監管機關。於第 13 條及第 14 條提供資訊之情形，控管者應將移轉及追求之合法利益通知資料主體。

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

2. 第 1 項第 1 款第 g 點之移轉不得涉及全部個人資料或登記內個人資料之所有分類。於由具合法利益者為諮詢而登記時，該移轉僅得依其請求或其為接收者之情形為之。

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

3. 第 1 項第 1 款第 a、b、及 c 點及第 2 款不適用於公務機關執行公權力之活動。

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

4. 第 1 項第 1 款第 d 點之公共利益應為歐盟法或控管者受拘束之會員國法所承認者。

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the

transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

5. 於欠缺充足程度保護之決定之情形下，歐盟或會員國法得基於公益之重要原因，明訂特殊類型之個人資料移轉至第三國或國際組織之限制。會員國應向執委會通知該等規定。

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

6. 控管者或處理者應於第 30 條所稱之紀錄中，記錄本條第 1 項第 2 款所稱評估及適當之保護。

Article 50 International cooperation for the protection of personal data

第五十條　個人資料保護之國際合作

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

對於第三國及國際組織，執委會及監管機關應採取適當之措施：

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(a) 發展國際合作機制以促進有效執行個人資料保護之立法；

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(b) 提供執行個人資料保護之立法上之國際互助，包括透過關於個人資料保護之適當措施與其他基本權利及自由之通知、申

訴轉介、調查協助及資訊交換；

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(c) 使利害關係人參與以進一步執行個人資料保護之立法上之國際合作為目標討論及活動；

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

(d) 提升個人資料保護立法與實務之交換與文件紀錄，包括與第三國之管轄衝突。

CHAPTER VI Independent supervisory authorities

第六章　獨立監管機關

Section 1 Independent status

第一節　獨立地位

Article 51 Supervisory authority

第五十一條　監管機關

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

1. 各會員國應設立至少一個獨立公務機關，職司本規則適用之監控，以保護當事人有關個人資料處理之基本權與自由及促進歐盟內個

人資料之自由流動（「監管機關」）。

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

2. 各監管機關應致力於本規則於歐盟之一致適用。為此，監管機關應依第七章之規定互相及與執委會合作。

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

3. 於一會員國內設立一個以上之監管機關時，該會員國應指定其一於委員會代表各監管機關，並應建立機制，以確保其他機關遵循與第 63 條所稱之一致性機制有關之規範。

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

4. 各會員國應於 2018 年 5 月 25 日前通報執委會其依本章所採行之法律條文，並應通報影響前揭法律條文之任何後續修正，不得遲延。

Article 52 Independence

第五十二條　獨立

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

1. 各監管機關應依本規則完全獨立行使職權。

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance

with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

2. 各監管機關之成員應依本規則行使職權，不受直接或間接之外部干擾，並不應依循任何人之指示。

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

3. 各監管機關之成員不得為與其職務不相容之行為，並不得於其任期內從事任何不相容之兼職，有無報酬不在所問。

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

4. 各會員國應確保各監管機關具備有效行使職權所需之人力、技術及財務資源、辦公室以及基礎設施，包括於委員會因互助、合作及參與所需執行者。

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

5. 各會員國應確保各監管機關選擇並擁有自身之員工，且員工應受該監管機關成員排他之指示。

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

6. 各會員國應確保各監管機關受財務控制，但不得影響其獨立，且應有單獨、公開之年度預算，並得作為國家或聯邦整體預算之一部分。

Article 53 General conditions for the members of the supervisory authority

第五十三條　監管機關成員之一般條款

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

1. 會員國應使其監管機關之各成員由下列單位本於透明程序所任命：

— their parliament;
— their government;
— their head of State; or
— an independent body entrusted with the appointment under Member State law.

— 國會；
— 政府；
— 國家元首；或
— 依會員國法委託設立之獨立機構。

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

2. 各成員應具行使職權之資格、經驗及技巧，特別是關於個人資料保護之領域。

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

3. 成員之職責應依各該會員國法於其任期結束、解任或強制退休時終止。

4. A member shall be dismissed only in cases of serious misconduct

or if the member no longer fulfils the conditions required for the performance of the duties.

4. 僅於有嚴重不當行為或成員不再符合執行職務之資格時，得解任成員。

Article 54 Rules on the establishment of the supervisory authority

第五十四條　監管機關設立之規則

1. Each Member State shall provide by law for all of the following:

1. 各會員國應以法律規定下列所有事項：

(a) the establishment of each supervisory authority;

(a) 各監管機關之設立；

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(b) 得受任命為各監管機關成員所需之資格與條件。

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(c) 任命各監管機關成員之規則與程序；

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(d) 各監管機關成員之任期不得少於四年。但為保障監管機關獨立性之必要而採取交錯任期之方式，使 2016 年 5 月 24 日後第一次任命之任期較短者，不在此限；

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(e) 各監管機關成員是否得受再任命，及若是，其任期數；

(f) the conditions governing the obligations of the member or

members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

(f) 各監管機關成員及工作人員之義務條款、禁止其任期內與任期後與其職務不相容之行為、兼職及利益、以及停職之規範。

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

2. 依歐盟或會員國法，各監管機關之成員及工作人員應於任期內及任期後，對因行使職權知悉之任何機密資料負專業保密義務。於任期內，其專業保密義務尤其應適用於本規則之當事人侵害報告。

Section 2 Competence, tasks and powers
第二節　權限、職務及權力

Article 55 Competence
第五十五條　權限

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

1. 各監管機關應有權於自己之會員國領域內依本規則執行指定之職務並行使權力。

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
2. 於公務機關或私人機構依第 6 條 1 項第 c 或 e 點執行處理時，有關之會員國監管機關應有權限。於該等情形，不適用第 56 條規定。
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.
3. 監管機關不應有權監督法院就其司法權所為之處理執行。

Article 56 Competence of the lead supervisory authority
第五十六條　領導監管機關之權限

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
1. 於不損及第 55 條之前提下，該控管者或處理者之主要分支機構或該單一分支機構之監管機關，應有權作為該控管者或處理者依第 60 條程序為跨境處理時之領導監管機關。
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
2. 如標的事項僅涉及該會員國之單一分支機構、或受嚴重影響之資料主體僅在該會員國時，各監管機關應有權處理提交至其之申訴、或對本規則可能之違反，不受第 1 項之限制。
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on

that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

3. 於本條第二項之情形，監管機關應通知領導監管機關該事項，不得無故延遲。領導監管機關應於受通知起三週內，決定是否依第 60 條之程序處理該事項，並應考量監管機關通知之會員國內是否有控管者或處理者之分支機構。

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

4. 於領導監管機關決定處理該事項時，應遵循第 60 條之程序。通知領導監管機關之監管機關得提交裁決草案至領導監管機關。領導監管機關於依第 60 條第 3 項擬訂裁決時，應盡可能考慮該草案。

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

5. 於領導監管機關決定不處理該事項時，通知領導監管機關之監管機關應依第 61 條及第 62 條處理。

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

6. 領導監管機關應為控管者或處理者於其執行跨境處理時，唯一之溝通對口。

Article 57 Tasks

第五十七條　職務

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

1. 於不損及本規則設立之其他職務之前提下，各監管機關應於其領域內：

(a) monitor and enforce the application of this Regulation;

(a) 監控及執行本規則之適用；

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(b) 提升公眾對有關處理之風險、規則、保護措施及權利之意識及理解。專門針對兒童之活動應受特別之注意；

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(c) 依會員國法建議國會、政府及其他機關或機構，關於涉及處理之當事人權利及自由保護之立法及行政措施；

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(d) 提升控管者及處理者對其於本規則之義務之意識；

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(e) 基於請求，提供關於本規則下權利行使之資料予任何資料主體，若適合，與其他會員國之監管機關合作提供；

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and

investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(f) 處理資料主體或機構、組織或協會依第 80 條之申訴，並適當程度調查該申訴事項，於合理時間內通知申訴人調查之進度與結果，尤其於進一步之調查或與其他監管機關之協調為必要時；

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(g) 與其他監管機關合作，包括分享資訊及互助，以確保本規則適用與執行之一致性；

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(h) 執行本規則適用之調查，包括其他監管機關或其他公務機關所提供資訊之基礎；

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(i) 於相關發展影響個人資料之保護時監控之，尤其是資訊與通訊科技與商業慣例之發展；

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(j) 通過第 28 條第 8 項及第 46 條第 2 項第 d 點所稱之定型化契約條款；

(k) establish and maintain a list in relation to the requirement for data

protection impact assessment pursuant to Article 35(4);

(k) 依第 35 條第 4 項設立並維持與資料保護影響評估之要求相關之清單；

(l) give advice on the processing operations referred to in Article 36(2);

(l) 提供第 36 條第 2 項所稱處理活動之建議；

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(m) 依第 40 條第 1 項鼓勵制定行為守則，並依第 40 條第 5 項提供意見及核准提供充足保護措施之行為守則；

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(n) 鼓勵依第 42 條第 1 項設立資料保護認證機制及資料保護標章與標誌，並依 42 條第 5 項核准認證之標準；

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(o) 於得適用時，依第 42 條第 7 項定期檢驗頒發之認證；

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(p) 草擬並公布第 41 條監督行為守則之機構及第 43 條認證機構之認證標準；

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) 進行第 41 條監督行為守則之機構及第 43 條認證機構之認證；

(r) authorise contractual clauses and provisions referred to in Article

46(3);

(r) 授權第 46 條第 3 項所稱之契約條款及規定；

(s) approve binding corporate rules pursuant to Article 47;

(s) 依第 47 條核准有拘束力之企業守則；

(t) contribute to the activities of the Board;

(t) 協助委員會之活動；

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(u) 依第 58 條第 2 項保存違反規則及採取措施之內部紀錄；及

(v) fulfil any other tasks related to the protection of personal data.

(v) 完成任何與個人資料保護相關之職務。

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

2. 各監管機關應透過諸如亦得單以電子方式完成而不須其他溝通方式之申訴提交表格等方式，促進第 1 項第 f 點之申訴提交。

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

3. 各監管機關之職務行使不應向資料主體收取費用，且於得適用時，亦不應向資料保護員收取之。

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

4. 於請求顯無理由或過量時，尤其於重複情形，監管機關得基於行政成本收取合理費用，或拒絕處理請求。監管機關應負請求顯無

理由或請求過量之舉證責任。

Article 58 Powers

第五十八條　權力

1. Each supervisory authority shall have all of the following investigative powers:

1. 各監管機關應有下列全部調查之權力：

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(a) 命令控管者、處理者，以及若有控管者或處理者之代表時，該等代表提供任何其執行任務所需之資訊；

(b) to carry out investigations in the form of data protection audits;

(b) 以資料保護查核之形式進行調查；

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(c) 進行依第 42 條第 7 項核發之認證的審查；

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(d) 對聲稱本規則被違反時通知控管者或處理者；

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(e) 自控管者或處理者獲得接近使用個人資料以及執行其任務所需之所有資訊；

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

(f) 依歐盟或會員國程序法，得進入控管者或處理者之任何辦公處所，包括接近使用任何資料處理設備及方式。

2. Each supervisory authority shall have all of the following corrective powers:

2. 各監管機關應有下列全部之糾正權力：

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(a) 當欲進行之資料處理可能會違反本規則之規定時，向控管者或處理者發布警告；

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(b) 當資料處理已違反本規則之規定時，對控管者或處理者發布告誡；

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(c) 命令控管者或處理者遵循資料主體行使其依本規則之權利的要求；

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(d) 命令控管者或處理者以適當之特定方法及於特定期間內使資料處理符合本規則之規定；

(e) to order the controller to communicate a personal data breach to the data subject;

(e) 命令控管者向資料主體通知個人資料之侵害；

(f) to impose a temporary or definitive limitation including a ban on processing;

(f) 課予暫時或終局之限制，包括對資料處理之禁令；

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the

notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(g) 命令依第 16 條、第 17 條及第 18 條對個人資料之更正或刪除，或對資料處理之限制，以及對個人資料依照第 17 條第 2 項及第 19 條被揭露之接收者就該等行動之通知；

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(h) 撤銷或命令認證機構撤銷依第 42 條及第 43 條所為之認證，或若認證之要件不具備或不再具備時，命令認證機構不得核發認證；

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(i) 依個案情形，額外或不以本項所提及之其他方式而依第 83 條處以行政罰鍰；

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(j) 命令對位於第三國之接收者或國際組織停止資料流通。

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

3. 各監管機關應有下列全部之授權及建議權力：

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(a) 依第 36 條之事前諮詢程序建議控管者；

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(b) 對國會、會員國政府、依會員國法對其他公共團體、機構及大眾主動或依請求發布針對任何與個人資料保護相關之議題的意見；

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(c) 若會員國法要求事前授權時，授權第 36 條第 5 項所述之資料處理；

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(d) 發布意見並核准第 40 條第 5 項所述之行為守則草案；

(e) to accredit certification bodies pursuant to Article 43;

(e) 依第 43 條委託認證機構；

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(f) 依第 42 條第 5 項發布認證並核准認證之標準；

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(g) 採用第 28 條第 8 項及第 46 條第 2 項第 d 點所述之標準資料保護條款；

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(h) 授權第 46 條第 3 項第 a 點所述之契約條款；

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(i) 授權第 46 條第 3 項第 b 點所述之行政安排；

(j) to approve binding corporate rules pursuant to Article 47.

(j) 依第 47 條核准有拘束力之企業守則。

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union

and Member State law in accordance with the Charter.

4. 監管機關行使本條賦予之權力應有適當保護措施，包括歐盟法及會員國法依憲章所規定之有效之司法救濟及正當程序。

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

5. 各會員國應有法律規定監管機關應有權力將本規則之違反檢送司法機關，並於適當時開啟或參與司法程序，以執行本規則之規定。

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

6. 各會員國應有法律規定其監管機關應有第 1 項、第 2 項及第 3 項以外之額外權力。該等權力之實行不應減損第七章之有效性。

Article 59 Activity reports
第五十九條　活動報告

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

各監管機關應編製年度活動報告，得包括受告知之侵害類型以及依第 58 條第 2 項採取之措施類型清單。該等報告應依會員國法之指定提交國會、政府及其他有權機關。該等報告應對大眾、執委會及委員會公開。

CHAPTER VII Cooperation and consistency

第七章　合作及一致性

Section 1 Cooperation

第一節　合作

Article 60 Cooperation between the lead supervisory authority and the other supervisory authorities concerned

第六十條　領導監管機關與其他相關監管機關間之合作

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

1. 領導監管機關應依本條與其他相關監管機關合作並致力於達成共識。領導監管機關及相關監管機關應彼此交換所有相關之資訊。

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

2. 領導監管機關得於任何時候請求其他相關監管機關依第 61 條提供互助，並得依第 62 條採行聯合作業，特別係為了進行調查，或為了監督關於在其他會員國設立之控管者或處理者之措施的施行。

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities

concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

3. 領導監督機關應將該事項之相關資訊傳送予其他相關監管機關，不得遲延。其應提交裁決草案予其他相關監管機關，不得遲延，以獲得其等之意見並適當考量其等之觀點。

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

4. 當任一其他相關監管機關在依本條第 3 項受諮詢後四週內表達對該裁決草案相關且合理之異議時，若領導監管機關不遵循該相關且合理之異議，或認為該異議不相關或不合理者，則應將該事項提交予第 63 條所述之一致性機制。

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

5. 當領導監管機關欲遵循該相關且合理之異議時，其應提交修訂裁決草案予其他相關監管機關以獲得其等之意見。該修訂裁決草案應受第 4 項所述程序之約束於兩週內為之。

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

6. 當無任何其他相關監管機關於第 4 項及第 5 項所述之期限內對領導監管機關所提交之裁決草案提出異議者，應視為領導監管機關及相關監管機關同意該裁決草案並應受其拘束。

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

7. 領導監督機關應依其情形通過該裁決並告知控管者或處理者之主要分支機構或單一分支機構，並向其他相關監管機關及委員會通知該裁決，包括扼要之相關事實及理由。受理申訴之監管機關應向申訴人通知該裁決。

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

8. 當申訴遭駁回或不予受理時，第 7 項之規定不適用之，受理申訴之監管機關應通過該裁決並將其告知申訴人，並應通知控管者。

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall

notify it to that complainant and shall inform the controller or processor thereof.

9. 若領導監管機關及相關監管機關同意駁回或不受理部分申訴而僅對部分申訴採取行動，則應對該事項之每個部分採取個別之裁決。領導監管機關應通過與控管者有關行動相關之裁決，且應將該裁決告知控管者或處理者之主要分支機構或單一分支機構，並應通知申訴人，而申訴人之監管機關應通過關於駁回或不受理該申訴部分之裁決，並應將該裁決告知申訴人且通知控管者或處理者。

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

10. 在依第 7 項及第 9 項受告知領導監管機關之裁決後，控管者及處理者應採取必要措施以確保其所有於歐盟境內之分支機構的處理活動皆有遵守該裁決。控管者或處理者應將為遵守該裁決所採取之措施告知領導監管機關，領導監管機關並應通知其他相關監管機關。

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

11. 若在特殊情況下，相關監管機關有理由認為有緊急必要採取行動以保護資料主體之利益者，應適用第 66 條所述之緊急程序。

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

12. 領導監管機關及其他相關監管機關應使用標準化格式，以電子方

式互相提供本條所需之資訊。

Article 61 Mutual assistance

第六十一條　互助

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

1. 監管機關應提供彼此相關資訊並互助以一致地實施並適用本規則，並應訂定相互有效合作之措施。互助應特別包括資訊要求及監督措施，例如要求進行事前授權及諮詢、檢查及調查。

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

2. 各監管機關應採取所有適當措施，不得無故遲延且不遲於收到請求後一個月內，回覆另一監管機關之請求。該等措施特別得包括傳送關於調查行為之相關資訊。

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

3. 請求協助應包含所有必要資訊，包括該請求之目的及理由。交換之資訊應僅得用於所請求之目的。

4. The requested supervisory authority shall not refuse to comply with the request unless:

4. 受請求之監管機關不得拒絕接受該請求，除非：
   (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
   (a) 其無權處理請求之標的或請求執行之措施；或
   (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.
   (b) 接受該請求將違反受請求之監管機關所應遵守之本規則、歐盟法或會員國法。
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
5. 受請求之監管機關應將結果或依其情形將採取之措施的進展狀況通知請求之監管機關，以回應該請求。受請求之監管機關應提供任何拒絕依第 4 項接受請求之理由。
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
6. 受請求之監管機關在一般情形應使用標準化格式，以電子方式提供其他監管機關請求之資訊。
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
7. 受請求之監管機關就其依互助之請求採取之任何行動不得收取費用。監管機關得同意就特別情況下提供互助產生之具體支出之互相補償規範。

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

8. 若監管機關不於收到另一監管機關之請求後一個月內提供本條第 5 項所述之資訊，請求之監管機關得依第 55 條第 1 項在該會員國領土內採取臨時措施。在該等情況下，應推定有依第 66 條第 1 項採取行動之迫切需要，並要求委員會依第 66 條第 2 項做出緊急且有拘束力之裁決。

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

9. 執委會得透過施行細則具體規範本條所述之互助的格式及程序，以及監管機關相互間及監管機關與委員會間以電子方式資訊交換之安排，特別是本條第 6 項所述之標準化格式。該施行細則應通過第 93 條第 2 項所述之檢驗程序。

Article 62 Joint operations of supervisory authorities
第六十二條　監管機關之聯合作業

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of

other Member States are involved.

1. 監管機關應斟酌情形採取聯合作業，包括聯合調查及聯合執行措施，即包含其他會員國之監管機關的成員或職員。

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

2. 若控管者或處理者在數個會員國有分支機構，或在一個以上會員國之大量資料主體可能受處理活動之實質影響，各會員國之監管機關應有權參加聯合作業。依第 56 條第 1 項或第 4 項之主管監管機關應邀請其中各會員國之監管機關參加聯合作業，並應立即回應監管機關參加之要求。

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

3. 監管機關得依會員國法及參加監管機關之授權對參加監管機關參

與聯合作業之成員或職員授予權力，包括調查權，或在主辦監管機關所屬會員國之法律許可之範圍內，允許參加監管機關之成員或職員依參加監管機關會員國法行使調查權。該等調查權僅得在主辦監管機關成員或職員之當面指導下執行。參加監管機關之成員或職員應遵守主辦監管機關之會員國法。

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

4. 若參加監管機關之職員依第 1 項在另一會員國工作者，對其在工作期間造成之任何損害，主辦監管機關所屬之會員國應依其等工作所在地之會員國法對其等之行為負擔責任，包括賠償責任。

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

5. 造成損害所在地之會員國應依適用其自身職員造成損害之條件，賠償該損害。參加監管機關之職員對其他會員國之任何人造成損害者，其所屬會員國應全額賠償該其他會員國向有權受償之人支付之任何金額。

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

6. 在不妨礙第三人行使權利之情況下，除第 5 項外，在第 1 項規定

之情形下，各會員國應不要求另一會員國賠償關於第 4 項所述之損害。

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

7. 如欲進行聯合作業，且監管機關未於一個月內遵守本條第 2 項後段所規定之義務，其他監管機關得依第 55 條在該會員國之領土上採取臨時措施。在該等情況下，應推定有依第 66 條第 1 項採取行動之迫切需要，並要求委員會依第 66 條第 2 項提出意見或做出緊急且有拘束力之裁決。

Section 2 Consistency
第二節　一致性

Article 63 Consistency mechanism
第六十三條　一致性機制

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

為有助於本規則於歐盟境內一致之適用，監管機關應透過本節所規定之一致性機制互相合作，並斟酌情形與執委會合作。

Article 64 Opinion of the Board

第六十四條　委員會之意見

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

1. 當主管監管機關欲採取下列任一措施時，委員會應發布其意見。為此，當有下列任一情形時，主管監管機關應向委員會通知該裁決草案：

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(a) 旨在採取依第 35 條第 4 項規定進行資料保護影響評估之處理活動清單；

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(b) 涉及依第 40 條第 7 項之事項，即行為守則草案或行為守則之修訂或擴充是否符合本規則；

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(c) 旨在核准第 41 條第 3 項之機構認證標準或第 43 條第 3 項之認證機構；

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(d) 旨在決定第 46 條第 2 項第 d 點及第 28 條第 8 項所述之標準資料保護條款；

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(e) 旨在授權第 46 條第 3 項第 a 點所述之契約條款；或

(f) aims to approve binding corporate rules within the meaning of Article 47.

(f) 旨在核准第 47 條定義下有拘束力之企業守則。

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

2. 任何監管機關、委員會主席或執委會主席為獲得意見得要求委員會審查任何在一個以上之會員國具有一般適用性或產生效力之事項，特別是當主管監管機關不遵守第 61 條互助之義務，或第 62 條聯合作業之義務時。

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

3. 在第 1 項及第 2 項所規定之情形，若委員會尚未對同一事項發表過意見，應就提交予其之事項發布意見。該意見應於八週內以委員會成員過半數多數決之方式通過之。考量標的之複雜性，該期限得延長六週。關於依第 5 項向委員會成員分發之第 1 項所述之裁決草案，未在主席所指定之合理期間內表示異議之成員應被視為同意該裁決草案。

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

4. 監管機關及執委會應以電子方式使用標準化格式傳送任何相關資訊，依其情形包括事實摘要、裁決草案、使訂定該等措施為必要之理由，以及其他相關監管機關之觀點，不得無故遲延。

5. The Chair of the Board shall, without undue, delay inform by electronic means:

5. 委員會之主席應以電子方式通知，不得無故遲延：

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(a) 曾依標準化格式向其傳送之任何相關資訊之委員會及執委會之成員。必要時，委員會之秘書應提供相關資訊之翻譯；以及

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

(b) 第 1 項及第 2 項所述之監管機關（視情況而定）及執委會之意見，並使其公開。

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

6. 主管監管機關不得在第 3 項所述期間通過其依第 1 項所述之裁決草案。

7. The supervisory authority referred to in paragraph 1 shall take utmost

account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

7. 第 1 項所述之監管機關應充分考量委員會之意見，並應在收到意見後兩週內，透過電子方式使用標準化格式向委員會主席通知是否維持或修訂其裁決草案，以及有修訂時，修訂之裁決草案。

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

8. 若相關監管機關在第 7 項所述之期限內通知委員會之主席其不欲遵循全部或部分委員會之意見，若有正當理由，應有第 65 條第 1 項之適用。

Article 65 Dispute resolution by the Board
第六十五條　委員會之爭議解決

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

1. 為確保本規則在個案中正確且一致之適用，在下列情況下，委員會應通過有拘束力之裁決：

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(a) 在第 60 條第 4 項所述之情況下，已有一相關監管機關對領導

監管機關之裁決草案提出相關且合理之異議，或領導監管機關已以不相關或不合理為由拒絕該等異議。該有拘束力之裁決應涉及該相關且合理之異議作為理由之所有事項，特別是是否違反本規則；

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(b) 相關監管機關對該主要分支機構是否有處理權限有爭議時；

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

(c) 當主管監管機關在第 64 條第 1 項所述情況下為請求委員會之意見，或不遵循委員會根據第 64 條發布之意見。在該等情況下，任何相關監管機關或執委會得將該等事項通知委員會。

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

2. 第 1 項所述之裁決應在委員會成員三分之二多數決之方式提交該待決標的後一個月內作成。該期限得考量待決標的之複雜性而延長一個月。第 1 項所述之裁決應合理並提交予領導監管機關以及所有相關監管機關，並對其等有拘束力。

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members

of the Board are split, the decision shall by adopted by the vote of its Chair.

3. 若委員會無法於第 2 項所述之期限內通過裁決，其應於第 2 項所述之第二個月期滿後之兩個星期內以委員會成員過半數多數決之方式通過其裁決。若委員會之成員意見分歧，該裁決應由其主席投票通過。

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

4. 相關監管機關不得在第 2 項及第 3 項所述之期間通過根據第 1 項提交予委員會之待決標的。

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

5. 歐洲資料委員會之主席應將第 1 項所述之裁決告知相關監管機關，不得無故遲延。其亦應通知執委會。該裁決應在監管機關依第 6 項所述通知最終裁決後立即在歐洲資料委員會之網站上公布。

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this

Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

6. 領導監管機關或受理申訴之監管機關（視情況而定）應根據本條第 1 項所述之裁決作出其最終裁決，不得無故遲延，且最遲應於委員會告知其裁決後一個月內為之。領導監管機關或受理申訴之監管機關（視情況而定）應將其分別通知控管者或處理者以及資料主體其最終裁決之日期通知委員會。相關監管機關之最終裁決應根據第 60 條第 7 項、第 8 項及第 9 項之規定通過。最終裁決應參照本條第 1 項所述之裁決，並應具體說明該項所述之裁決將依本條第 5 項之規定在委員會之網站上公布。最終裁決應附有本條第 1 項所述之裁決。

Article 66 Urgency procedure
第六十六條　緊急程序

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

1. 在特殊情況下，當相關監管機關認為有迫切需要採取行動以保護資料主體之權利及自由，其得不適用第 63 條、第 64 條及第 65 條所述之一致性機制，或第 60 條所述之程序，而立即採取旨在其所在國境內產生法律效果，且有效期限不得超過三個月之臨時措施。

監管機關應立即向其他相關監管機關、委員會及執委會通知該等措施及採取該等措施之理由。

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

2. 如監管機關已依第 1 項採取措施，且認為需緊急通過最終措施者，其得請求委員會提出緊急意見或緊急且有拘束力之裁決，並說明請求該等意見或裁決之理由。

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

3. 若主管監管機關在有採取行動之迫切需要時沒有採取適當措施，任何監管機關得依其情形向委員會請求緊急意見或緊急且有拘束力之裁決，以保護資料主體之權利及自由，並說明請求該等意見或裁決之理由，包括採取行動之迫切需要。

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

4. 本條第 2 項及第 3 項所述之緊急意見或緊急且有拘束力之裁決應在兩週內以委員會成員過半數多數決之方式通過，而不適用第 64 條第 3 項及第 65 條第 2 項。

Article 67 Exchange of information

第六十七條　資訊交換

The Commission may adopt implementing acts of general scope in order

to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.
執委會得通過一般範圍內之施行法以具體化規範監管機關相互間及監管機關與委員會間以電子方式資訊交換的安排，特別是第 64 條所述之標準化格式。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).
該等施行法應經第 93 條第 2 項所述之檢驗程序通過。

Section 3 European data protection board
第三節　歐洲資料保護委員會

Article 68 European Data Protection Board
第六十八條　歐洲資料保護委員會

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.
1. 茲此設立歐洲資料保護委員會（「委員會」），為歐盟之機構，並應具有法人格地位。
2. The Board shall be represented by its Chair.
2. 委員會應以其主席為代表。
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
3. 委員會應由各會員國監管機關及歐盟資料保護監督組織之首長或其等相應之代表組成。
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance

with that Member State's law.

4. 若在一會員國內有超過一個監管機關負責監督本規則條款之適用，應根據會員國法任命一名聯合代表。

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

5. 執委會應有權參加委員會之活動及會議，但無表決權。執委會應指定一名代表。委員會之主席應向執委會通知委員會之活動。

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

6. 在第 65 條之情形，歐盟資料保護監督組織應僅對涉及適用歐盟當局、機構、辦事處及局處且實質上符合本規則之原則與規定的裁決有表決權。

Article 69 Independence

第六十九條　獨立性

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

1. 委員會依第 70 條及第 71 條執行其任務或行使其權力時，應獨立行使職權。

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

2. 在不影響第 70 條第 1 項第 b 點及第 70 條第 2 項所述執委會提出請求之情況下，委員會在執行其任務或行使其權力時不得尋求或採取任何人之指示。

Article 70 Tasks of the Board

第七十條　委員會之任務

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

1. 委員會應確保本規則之一致適用。為此目的，委員會特別應主動或斟酌情形在執委會之要求下為下列行為：

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(a) 監督並確保本規則在第 64 條及第 65 條規定情形之正確適用，但不妨礙國家監管機關之任務；

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(b) 就與歐盟境內個人資料保護之任何議題，包括就本規則之任何建議修訂，向執委會提供意見；

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(c) 就控管者、處理者及監管機關對於有拘束力之企業守則的資訊交換格式及程序，向委員會提供意見；

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(d) 發布第 17 條第 2 項所述自公開通訊服務刪除個人資料連結、複製或仿製之指導原則、建議及最佳做法；

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering

the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(e) 主動或依其一名成員或執委會之請求，審查涵蓋本規則適用之任何問題並發布指導原則、建議及最佳做法以鼓勵本規則之一致適用。

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(f) 為進一步規範根據第 22 條第 2 項建檔之標準與條件，依本項第 e 點發布指導原則、建議及最佳做法；

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(g) 就確定個人資料侵害並決定第 33 條第 1 項及第 2 項所述之無故遲延，以及控管者或處理者被要求通知該個人資料侵害之特定情況，依本項第 e 點發布指導原則、建議及最佳做法；

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(h) 在第 34 條第 1 項所述就個人資料侵害可能導致對當事人權利及自由之高風險之情形，依本項第 e 點發布指導原則、建議及最佳做法。

(i) issue guidelines, recommendations and best practices in

accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(i) 基於控管者遵循之有拘束力之企業守則及處理者遵循之有拘束力之企業守則，並基於進一步必要之要求，為進一步規範個人資料移轉之標準及依第 47 條之要求以確保相關資料主體個人資料之保護，依本項第 e 點發布指導原則、建議及最佳做法；

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(j) 為根據第 49 條第 1 項進一步規範個人資料移轉之標準及要求，依本項第 e 點發布指導原則、建議及最佳做法；

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(k) 就第 58 條第 1 項、第 2 項及第 3 項所述措施之適用，以及第 83 條罰鍰之訂定，為監管機關制定指導原則；

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(l) 審查第 e 點及第 f 點所述指導原則、建議及最佳做法之實際適用；

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing

common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(m) 就第 54 條第 2 項當事人報告本規則侵害之一般程序之建立，依本項第 e 點發布指導原則、建議及最佳做法；

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(n) 依第 40 條及第 42 條鼓勵行為守則之訂定及資料保護認證機制、資料保護標章及標誌之建立；

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(o) 依第 43 條進行認證機構之委託及其定期檢驗，並維護依第 43 條第 6 項受託機關及依 42 條第 7 項設立於第三國之受託控管者或處理者的公共紀錄；

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(p) 為第 42 條認證機構之委託，具體化規範第 43 條第 3 項所述之要求；

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(q) 提供執委會關於第 43 條第 8 項所述認證要求之意見；

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(r) 提供執委會關於第 12 條第 7 項所述標誌方式之意見；

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether

a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(s) 提供執委會關於第三國或國際組織保護程度適當性之評估，包括評估第三國、第三國內之領域或特定部門、或國際組織是否不再確保適當程度之保護。為此，執委會應提供委員會所有必要之文件，包括與第三國政府關於第三國、第三國內之領域或部門，或與國際組織之通信。

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(t) 依據第 64 條第 1 項所述之一致性機制發布對監管機關裁決草案之意見，發布對第 64 條第 2 項提交事項之意見，以及依第 65 條發布有拘束力之裁決，包括第 66 條所述之情形；

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(u) 促進監管機關間之合作、有效之雙邊及多邊資訊交換及最佳做法；

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(v) 促進一般培訓方案並促進監管機關間及在適當時與第三國之

監管機關或國際組織之人員交換；

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(w) 促進與全世界之資料保護監管機關間資料保護立法及實踐知識及文件之交換。

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(x) 發布對根據第 40 條第 9 項以歐盟層級起草之行為守則的意見；及

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

(y) 維護一大眾得接近使用之電子紀錄，紀錄監管機構及法院於一致性機制中處理之議題所做之裁決。

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

2. 若執委會要求委員會提供建議，考量該事項之急迫性，得指定一定之時限。

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

3. 委員會應將其意見、指導原則、建議及最佳做法轉呈執委會及第 93 條所述之委員會，並將其公開。

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

4. 委員會應在適當時諮詢利害關係人，並給予其等在合理期間內陳述意見之機會。在不影響第 76 條之情況下，委員會應公布諮詢程

序之結果。

Article 71 Reports

第七十一條　報告

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

1. 委員會應編製關於歐盟境內資料處理當事人保護之年度報告，以及相關時於第三國及國際組織之資料處理。此報告應公開並提交歐洲議會、歐洲理事會及執委會。

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

2. 年度報告應包括對第 70 條第 1 項第 1 點所述之指導原則、建議及最佳做法之實際適用，以及第 65 條所述有拘束力之裁決之審查。

Article 72 Procedure

第七十二條　程序

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

1. 除本規則另有規定，委員會應以其成員過半數多數決做出裁決。

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

2. 委員會應以其成員三分之二多數決通過自己之議事規則，並組織自己之營運安排。

Article 73 Chair

第七十三條　主席

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
1. 委員會應以其成員過半數多數決選出一名主席及兩名副主席。
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.
2. 主席及副主席之任期為五年，得連任一次。

Article 74 Tasks of the Chair

第七十四條　主席之任務

1. The Chair shall have the following tasks: (a) to convene the meetings of the Board and prepare its agenda; (b)to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned; (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.
1. 主席應有下列任務：(a) 召開委員會會議並編製其議程；(b) 向領導監管機關及相關監管機關告知委員會依第 65 條通過之裁決；(c) 確保及時執行委員會之任務，特別是有關第 63 條所述之一致性機制者。
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.
2. 委員會應在其議事規則中規定主席及副主席間之任務分配。

Article 75 Secretariat

第七十五條　秘書處

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
1. 委員會應設置秘書處，且應由歐盟資料保護監督組織提供。

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
2. 秘書處僅得依委員會主席之指示執行其任務。
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
3. 參與執行本規則賦予委員會之任務的歐盟資料保護監督組織職員，其應遵循之報告管道，應與參與賦予歐盟資料保護監督組織之任務的職員遵循之報告管道有所區別。
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
4. 在適當情況下，委員會及歐盟資料保護監督組織應制訂並公布實行本條之諒解備忘錄，決定其等合作之條款，並適用於參與本規則賦予委員會之任務的歐盟資料保護監督組織職員。
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
5. 秘書處應提供分析、行政以及後勤之協助。
6. The secretariat shall be responsible in particular for:
6. 秘書處應特別負責：
   (a) the day-to-day business of the Board;
   (a) 委員會之日常業務；
   (b) communication between the members of the Board, its Chair and the Commission;
   (b) 委員會成員、主席及執委會間之溝通；
   (c) communication with other institutions and the public;

(c) 與其他機構及大眾之溝通；

(d) the use of electronic means for the internal and external communication;

(d) 使用電子方式進行內部及外部溝通；

(e) the translation of relevant information;

(e) 相關資訊之翻譯；

(f) the preparation and follow-up of the meetings of the Board;

(f) 準備及追蹤委員會會議；

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

(g) 準備、草擬並公布對監管機關間爭議解決之意見、裁決，及其他委員會通過之案文。

Article 76 Confidentiality

第七十六條　保密性

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

1. 委員會根據其議事規則，當認為有必要時，委員會之討論應保密。

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council[3].

2. 接近使用提交予委員會成員、專家及第三方代表之文件應遵守歐洲議會及歐盟理事會之歐盟規則第 1049/2001 號 [3] 之規定。

[3] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).
歐洲議會及歐盟理事會於 2001 年 5 月 30 日就公眾接近使用歐洲議會、歐盟理事會及執委會文件，制定歐盟規則第 1049/2001 號（官方公報 L 類第 145 期，2001 年 5 月 31 日，第 43 頁）。

CHAPTER VIII Remedies, liability and penalties

第八章　救濟、義務及處罰

Article 77 Right to lodge a complaint with a supervisory authority

第七十七條　向監管機關提出申訴之權利

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

1. 在不影響任何其他行政或司法救濟之情況下，如資料主體認為與其有關之個人資料處理違反本規則者，資料主體應有權向監管機關提出申訴，尤其係向其住所地、工作地或受侵害地之會員國。

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

2. 受理申訴之監管機關應通知申訴人申訴之過程及結果，包括依第 78 條規定提起司法救濟之可能性。

Article 78 Right to an effective judicial remedy against a supervisory authority

第七十八條　對監管機關提起有效司法救濟之權利

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

1. 在不影響任何其他行政或非司法救濟之情況下，自然人或法人應有權對監管機關就其所為具有法律拘束力之處分提起有效司法救濟。
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
2. 在不影響任何其他行政或非司法救濟之情況下，如第 55 條及第 56 條所定之監管主管機關不處理申訴或未於三個月內依照第 77 條規定通知申訴人申訴進展或結果者，資料主體應有權提起有效之司法救濟。
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
3. 對監管機關之訴訟應提交於監管機關設立地之會員國法院。
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.
4. 在委員會於一致性機制中提出意見或做出決定以前，已對監管機關所為處分提起訴訟者，監管機關應將該意見或決定轉交法院。

Article 79 Right to an effective judicial remedy against a controller or processor

第七十九條　對於控管者或處理者提出有效司法救濟之權利

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory

authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

1. 在不影響任何現有之行政或非司法救濟（包括依第 77 條向監管機關提出申訴之權利）之情況下，如資料主體認為其依本規則所定之權利因未遵守本規則處理其個人資料而遭受侵害者，資料主體應有權提出有效之司法救濟。

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

2. 對於控管者或處理者提起之訴訟應提交至該控管者或處理者設有分支機構之會員國法院。此外，除控管者或處理者係行使公權力之公務機關外，亦可向資料主體住所地之會員國法院提起之。

Article 80 Representation of data subjects

第八十條　資料主體之代表

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

1. 資料主體應有權委任依會員國法合法設立、以公益為目的，且在個人資料保護領域活躍之非營利機構、組織或社團，代其向監管機關提出申訴、代其行使第 77、78 及 79 條所定之權利，以及於會員國法有規定時，代其行使第 82 條所定收受賠償金之權利。

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

2. 會員國得規範本條第 1 項所定之任何機構、組織或社團，在該會員國境內享有受資料主體委任，向主管監管機關獨立提出第 77 條所定之申訴之權利，以及在有理由認為資料主體之權利因違反本規則之個人資料處理而受有損害時，行使第 78 條及第 79 條所定之權利。

Article 81 Suspension of proceedings

第八十一條　停止訴訟程序

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

1. 如會員國之管轄法院知悉關於同一控管者或處理者處理之同一事件已在其他會員國法院在案審理者，其應與他會員國之法院聯繫，以確認該訴訟之存在。

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first

seized may suspend its proceedings.

2. 如同一控管者或處理者處理之同一事件之訴訟程序已在他會員國的法院在案審理，除管轄在先以外之其他任何管轄法院得停止其訴訟程序。

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

3. 該等訴訟程序於第一審程序中在案審理，如管轄在先之法院就該等訴訟程序有管轄權，且其法律允許合併訴訟者，除管轄在先之法院外，任何其他法院亦得應一方當事人的聲請，拒絕管轄。

Article 82 Right to compensation and liability

第八十二條　賠償請求權及義務

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

1. 因違反本規則而遭受物質上或非物質上之損害時，任何人應有權利自控管者或處理者就其損害獲得賠償。

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

2. 任何涉及資料處理之控管者應對違反本規則之資料處理造成之損害承擔責任。僅在處理者未遵循本規則針對處理者所規定之義務，或其行為超出或違反控制者合法之指示時，處理者應對資料處理造成之損害承擔責任。

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

3. 若控管者或處理者可證明其等對於造成損害之事件不可歸責時，其等應免除第 2 項之責任。

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

4. 若有超過一個控管者或處理者，或控管者和處理者皆同時涉及同一資料處理，且依第 2 項及第 3 項應對造成損害之資料處理承擔責任時，每個控管者或處理者皆應對整個損害承擔責任以確保對資料主體有效之賠償。

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

5. 若控管者或處理者依第 4 項就所受損害為全部之賠償，則該控管者或處理者應有權依照第 2 項所規定之條件向其他涉及同一資料處理之控管者或處理者請求償還其等各自就該損害應分擔之部分。

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

6. 為行使受償之權利而進行之法院程序，應向第 79 條第 2 項所述會員國法下有管轄權之法院提起之。

Article 83 General conditions for imposing administrative fines

第八十三條　裁處行政罰鍰之一般要件

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

1. 依本條規定對於違反本規則處以第 4 項、第 5 項及第 6 項所定之行政罰鍰者，各監管機關應確保於個案中係有效、適當且具懲戒性。

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

2. 依個案情形，行政罰鍰應附加或取代第 58 條第 2 項第 a 至 h 點及第 j 點所定措施。於個案中決定是否處以行政罰鍰及決定其數額時，應考慮下列因素：

   (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

   (a) 違規之性質、嚴重性及持續期間，並考量到處理之性質範圍或目的，以及受影響之資料主體人數及其受損程度；

   (b) the intentional or negligent character of the infringement;

   (b) 違規之故意或過失；

   (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

   (c) 控管者或處理者所採減少資料主體損害之任何行為；

   (d) the degree of responsibility of the controller or processor taking

into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(d) 控管者或處理者之責任程度，並考量到其依第 25 條及第 32 條所實施之技術上及組織上之措施；

(e) any relevant previous infringements by the controller or processor;

(e) 控管者或處理者先前任何相關之違規情事；

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(f) 與監管機關之配合程度，以糾正其違規及減輕其違規所可能造成之不利影響；

(g) the categories of personal data affected by the infringement;

(g) 違規所影響之個人資料類型；

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(h) 監管機關知悉其違規之方式，尤其是控管者或處理者是否通知該違規或其通知之程度；

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(i) 先前已依照第 58 條第 2 項規定命控管者或處理者就同一標的採取措施者，該等措施之遵循；

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(j) 第 40 條所定經核准之行為守則或依第 42 條所定經核准之認證機制之遵循；及

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(k) 任何其他適用於該個案情形之加重或減輕因素，例如因違約而直接或間接獲得之經濟利益或避免之損失；

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

3. 對於相同或相關之處理作業，如控管者或處理者因故意或過失違反本規則之數個規定者，行政罰鍰總額不得超過最嚴重違規情事所定之數額。

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

4. 依照第二項規定，違反下列規定者，最高處以 10,000,000 歐元之行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之二，並以較高者為準：

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(a) 第 8 條、第 11 條、第 25 條至第 39 條及第 42 條及第 43 條所定控管者及處理者之義務；

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(b) 第 42 條及第 43 條所定認證機構之義務；

(c) the obligations of the monitoring body pursuant to Article 41(4).

(c) 第 41 條第 4 項所定監管機構之義務。

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

5. 依照第二項規定，違反下列規定者，最高處以 20,000,000 歐元之

行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之四，並以較高者為準：

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(a) 第 5 條、第 6 條、第 7 條及第 9 條所定處理之基本原則，包括同意之條件；

(b) the data subjects' rights pursuant to Articles 12 to 22;

(b) 第 12 至 22 條所定資料主體之權利；

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(c) 第 44 條至第 49 條所定個人資料移轉至第三國或國際組織之接收者；

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(d) 依照第 9 章通過之會員國法律所定之任何義務；

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

(e) 違反監管機關依第 58 條第 2 項規定之命令或暫時性或終局性之處理限制或停止資料傳輸，或未提供進入而違反第 58 條第 1 項規定；

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6. 違反監管機關依第 58 條第 2 項規定之命令者，依照本條第 2 項規定，最高處以 20,000,000 歐元之行政罰鍰，或如為企業者，最高達前一會計年度全球年營業額之百分之四，並以較高者為準。

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

7. 在不損及監管機關依第 58 條第 2 項所定糾正權力之情況下，各會員國得制定是否及如何對設立於該會員國之公務機關及機構處以行政罰之規定。

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

8. 監管機關依本條規定實施權力者，應遵守歐盟法及會員國法律，採取適當程序保障，包括有效之司法救濟及正當程序。

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

9. 如會員國之法律體系未規範行政罰鍰，而該體系確保有效之司法救濟且監管機關所裁處之行政罰鍰具有相同效力者，本條規定得由主管監管機關裁處之，並由國內管轄法院執行。無論如何，該等罰鍰應有效、適當且具懲戒性。該等會員國應於 2018 年 5 月 25 日前將其依本項規定通過之法律規定及任何後續之修法或影響該等規定之修正案通知執委會，不得遲延。

Article 84 Penalties

第八十四條　罰則

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

1. 會員國應制定違反本規則所適用之其他罰則之規定，尤其係依第 83 條不受行政罰鍰拘束之侵權行為，並應採取一切必要措施確保該等規範得予執行。該罰則應有效、適當且具懲戒性。

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

2. 各會員國應於 2018 年 5 月 25 日前將其依第 1 項規定通過之法律規定及任何後續影響該等規定之修正案通知執委會，不得遲延。

CHAPTER IX Provisions relating to specific processing situations

第九章　特殊處理情況之規範

Article 85 Processing and freedom of expression and information

第八十五條　處理與言論及資訊自由

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

1. 會員國應立法調和本規則所定個人資料保護之權利及表意自由與

資訊自由，包括新聞目的及學術、藝術及或文學表意目的之處理。

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

2. 基於新聞目的或學術、藝術或文學表意目的所為之處理，會員國為平衡個人資料保護及表意及資訊自由權利而有必要者，應除外於或豁免於第二章（原則）、第三章（資料主體之權利）、第四章（控管者及處理者）、第五章（個人資料移轉至第三國或國際組織）、第六章（獨立監管機關）、第七章合作及一致性）及第九章（特殊資料處理）所定規定。

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

3. 會員國應將其依第 2 項規定通過之法律規定及任何後續之修法或影響該等規定之修正案通知執委會，不得遲延。

Article 86 Processing and public access to official documents

第八十六條　官方文件之處理與公眾接近使用

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the

protection of personal data pursuant to this Regulation.
公務機關或公務機構或私人機構為履行公共利益而執行職務所持有並存在於官方文件之個人資料，得由該公務機關或機構依其所受拘束之歐盟法或會員國法律規定揭露予同受拘束之公務機關或機構，以調和公眾接近使用官方文件與本規則所定個人資料保護之權利。

Article 87 Processing of the national identification number
第八十七條　國民身分證字號之處理

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.
會員國得進一步決定就國民身分證字號或任何其他通用識別碼處理之特定條件。國民身分證字號或任何其他通用識別碼僅應於依據本規則已對資料主體之權利及自由為適當保護措施時始得使用之。

Article 88 Processing in the context of employment
第八十八條　僱傭關係下之處理

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment

relationship.

1. 會員國得以法律或團體協約規範更具體化規定，以確保僱傭關係下涉及員工個人資料處理之權利及自由，尤其是為徵才目的、包括履行法律或團體協約所規定之義務等之僱傭契約之履行、工作之管理、計畫及組織、工作場所之平等與多元性、工作之健康與安全、員工或客戶財產之保護，及個人或團體與僱傭有關之權利及福利之行使及享有之目的，以及終止僱傭關係之目的。

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

2. 該等規定應包括適當及具體措施，以確保資料主體之人性尊嚴、正當利益及基本權，尤其係關於處理之透明度、企業集團間或從事聯合經濟活動之企業團體間在工作場合中之個人資料移轉。

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

3. 各會員國應於 2018 年 5 月 25 日前將其依第 1 項規定通過之法律規定及任何後續影響該等規定之修正案通知執委會，不得遲延。

Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

第八十九條　為實現公共利益、科學或歷史研究目的或統計目的所為處理之保護措施及例外規定

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the

rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

1. 為實現公共利益、科學或歷史研究目的或統計目的之處理，應受本規則為資料主體之權利及自由所定適當保護措施之拘束。該等保護措施應確保已備妥技術上及組織上之措施，特別是用以確保資料最少蒐集原則之落實。只要上開目的得以實現，措施得包括假名化。當透過進階處理得實現上開目的，且進階處理不允許或不再允許識別資料主體者，上開目的應以該方式實現。

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

2. 為科學或歷史研究目的或統計目的處理個人資料者，歐盟法或會員國法得就第 15 條、第 16 條、第 18 條及第 21 條所定之權利訂定例外規定，但須符合本條第一項所定要件及保護措施，且該權利不可能或不會嚴重損害特定目的之實現，且該等例外係為實現上開目的所必要者。

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in

so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. 為實現公共利益處理個人資料者，歐盟法或會員國法得就第 15 條、第 16 條、第 18 條、第 19 條、第 20 條及第 21 條所定之權利訂定例外規定，但須符合本條第一項所定要件及保護措施，且該權利不可能或不會嚴重損害特定目的之實現，且該等例外係為實現上開目的所必要者。

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

4. 第 2 項及第 3 項所定之處理同時適用於不同目的者，該例外規定僅適用於該項規定所定目的之處理。

Article 90 Obligations of secrecy
第九十條　保密義務

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

1. 針對控管者或處理者依歐盟或會員國法或國內主管機構所訂規則負有職業或其他相應之保密義務，且調和個人資料保護權利與保密義務係適當且有必要者，會員國得就第 58 條第 1 項第 e 點及第 f 點所定監管機關之權利，訂定具體化規定。該等規定僅適用於控

管者或處理者已因該保密義務所涵蓋之活動中接收或取得個人資料。

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

2. 各會員國應於 2018 年 5 月 25 日前將其依第 1 項通過之規定及任何後續影響該規定之修正案通知執委會，不得遲延。

Article 91 Existing data protection rules of churches and religious associations

第九十一條　教會及宗教組織現存之資料保護規定

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

1. 會員國境內之教會及宗教組織或社團於本規則生效時所適用關於保護當事人資料處理之一般性規範，得繼續適用，但以該等規定符合本規則者為限。

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

2. 適用本條第一項所定一般性規範之教會及宗教組織，應受獨立監管機關之監督，該獨立監管機關得為專設機關，但以符合本規則第六章所定要件者為限。

CHAPTER X Delegated acts and implementing acts

第十章　授權法及施行法

Article 92 Exercise of the delegation

第九十二條　授權之行使

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

1. 依本條所定之條件，賦予執委會通過授權法之權力。

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

2. 第 12 條第 8 項及第 43 條第 8 項所述之權力應自 2016 年 5 月 24 日起在一段時間內授權予執委會。

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

3. 第 12 條第 8 項及第 43 條第 8 項所述之授權得由歐洲議會或歐盟理事會隨時廢止之。廢止之決定應終結該決定所載之授權。其應自公布於歐洲聯盟官方公報之日起或公布後之某日起生效。其不應影響任何已生效之授權行為的效力。

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

4. 委員會一經通過一項授權法，即應同時告知歐洲議會及歐盟理事會。

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.
5. 依第 12 條第 8 項及第 43 條第 8 項通過之授權法，應僅有在歐洲議會或歐盟理事會皆未在受通知後三個月內表示反對，或在該期限屆滿前歐洲議會及歐盟理事會皆通知執委會其等不會反對之情況下生效。該期限應依歐洲議會或歐盟理事會之提議延長三個月。

Article 93 Committee procedure

第九十三條　執委會之程序

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
1. 執委會應由一委員會協助。該委員會應為一歐盟規則第 182/2011 號意義上之委員會。
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
2. 於本項情形，歐盟規則第 182/2011 號第 5 條應適用之。
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.
3. 於本項情形，歐盟規則第 182/2011 號第 8 條與第 5 條應一同適用之。

CHAPTER XI Final provisions

第十一章　最終條款

Article 94 Repeal of Directive 95/46/EC

第九十四條　歐盟指令第 95/46/EU 號之廢止

1. Directive 95/46/EC is repealed with effect from 25 May 2018.
1. 歐盟指令第 95/46/EC 號自 2018 年 5 月 25 日起廢止。
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.
2. 凡提及該廢止指令者，應被解釋為係指本規則。涉及歐盟指令第 95/46/EC 號第 29 條所設立之個人資料處理保護小組應被解釋為係指依本規則所設立之歐洲資料保護委員會。

Article 95 Relationship with Directive 2002/58/EC

第九十五條　與歐盟指令第 2002/58/EC 號之關係

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

關於其等應遵守歐盟指令第 2002/58/EC 號之事項，本規則不得對自然人或法人施加與在歐盟公共通信網絡中提供公共電子通信服務有關之額外義務。

Article 96 Relationship with previously concluded Agreements

第九十六條　與已締結之協議之關係

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

會員國於 2016 年 5 月 24 日以前締結涉及個人資料移轉至第三國或國際組織，並遵守適用於該日期以前適用之會員國法之國際協議者，其應繼續有效，直到修正、被取代或被廢止。

Article 97 Commission reports

第九十七條　執委會報告

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

1. 2020 年 5 月 25 日以前，以及往後每四年，執委會應向歐洲議會及歐盟理事會提交關於評價及審查本規則之報告。該等報告應公開。

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

2. 在第 1 項所述評價及審查之範圍內，執委會應特別檢驗下列各點之適用與運作情形：

   (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

   (a) 關於第五章，即將個人資料移轉至第三國或國際組織，特別係根據本規則第 45 條第 3 項通過之裁決以及基於歐盟指令第

95/46/EC 號第 25 條第 6 項通過之裁決者；

(b) Chapter VII on cooperation and consistency.

(b) 第七章之合作及一致性。

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

3. 為第 1 項之目的，執委會得向會員國及監管機關請求資訊。

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

4. 在進行第 1 項及第 2 項所述之評價及審查時，執委會應考量歐洲議會、歐盟理事會及其他相關機構或來源之立場及調查結果。

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

5. 如有必要，執委會應提交適當之提案以修訂本規則，特別是考量資訊科技之發展，以及資訊社會之進展狀況。

Article 98 Review of other Union legal acts on data protection

第九十八條　對其他資料保護歐盟法案之審查

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

適當時，執委會應提交修訂其他關於個人資料保護歐盟法案之修法提案，以確保對當事人有關資料處理統一及一致之保護。此尤應涉及就

歐盟當局、機構、辦事處及局處之資料處理以及該等資料之流通，關於當事人保護之規範。

Article 99 Entry into force and application

第九十九條　生效及適用

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

1. 本規則應在公布於歐洲聯盟官方公報後之第 20 日起生效。

2. It shall apply from 25 May 2018.

2. 其應自 2018 年 5 月 25 日起適用。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

本規則應具有全面之拘束力，並應直接適用於所有會員國。

Done at Brussels, 27 April 2016.

完成於布魯塞爾，2016 年 4 月 27 日。

For the European Parliament	*For the Council*
歐洲議會	歐盟理事會
The President	*The President*
主席	主席
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

DIRECTIVES

指令

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

於 2016 年 4 月 27 日
歐洲議會及歐盟理事會之歐盟指令第 2016/680 號
為保護自然人(*)於主管機關基於預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的之個人資料處理及為該等資料之自由流通
廢止理事會框架決定第 2008/977/JHA 號

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

---

* 譯者註：原文多處使用 the protection of natural persons with regard to the processing of their personal data 一語，如加以直譯，固指自然人之個人資料保護，惟參照我國個人資料保護法之法規名稱及其第 2 條第 9 款將個人資料之本人稱為當事人的規定，以下就 natural person(s) 依其脈絡不特別翻譯，或翻譯為自然人或當事人或個人。

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the Committee of the Regions[1],
Acting in accordance with the ordinary legislative procedure[2],
Whereas:
歐盟所屬歐洲議會及歐盟理事會，根據
歐洲聯盟運作條約，特別是第 16 條第 2 項規定，
歐盟執行委員會之提案，
將立法草案交由會員國國會後，根據
歐洲區域委員會之意見 [1]，
依據通常的立法程序 [2]，
鑑於：

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(1) 個人資料處理之保護乃基本權。歐洲聯盟基本權利憲章（下稱憲章）第 8 條第 1 項及歐洲聯盟運作條約（即 TFEU）第 16 條

---

1 OJ C 391, 18.12.2012, p. 127.
官方公報 C 類第 391 期，2012 年 12 月 18 日，第 127 頁。

2 Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
歐洲議會於 2014 年 3 月 12 日所持立場（尚未刊載於官方公報）及理事會於 2016 年 4 月 8 日一讀所持立場（尚未刊載於官方公報）。歐洲議會於 2016 年 4 月 14 日所持立場。

第 1 項規定，任何人有保護其個人資料之權利。

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(2) 個人資料處理之保護原則與規則為應尊重其基本權及自由，尤其是其保護個人資料之權利，而不問其國籍或住居所。本指令旨在實現一個自由、安全及公義之區域。

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(3) 快速的科技發展及全球化對於個人資料之保護帶來了新的挑戰。蒐集與共享個人資料之規模已顯著提升。科技使個人資料以前所未有的規模受到處理，以進行如預防、調查、偵查及追訴刑事犯罪或執行刑罰等活動。

(4) The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed

by strong enforcement.

(4) 為達預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的，包括為維護及預防此等資料對歐盟內公共安全及個人資料自由流通造成之威脅，在主管機關間個人資料之自由流通及該等個人資料向第三國或國際組織之移轉應受促進，並同時確保個人資料之高度保護。此等發展需在歐盟內建構強力且更一致之資料保護框架，並落實執法。

(5) Directive 95/46/EC of the European Parliament and of the Council [3] applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

(5) 歐洲議會及歐盟理事會之歐盟指令第 95/46/EC 號 3 適用於會員國內公私部門之所有個人資料處理。然而，其不適用於共同體法律範圍之外的活動過程中所涉之個人資料處理，例如刑事事務之司法合作及警方合作領域之活動。

(6) Council Framework Decision 2008/977/JHA[4] applies in the areas of judicial cooperation in criminal matters and police cooperation. The

---

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
歐洲議會及歐盟理事會於 1995 年 10 月 24 日為保護個人有關個人資料處理及自由流通制定歐盟指令第 95/46/EC 號（官方公報 L 類第 281 期，1995 年 11 月 23 日，第 31 頁）。

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).
2008 年 11 月 27 日為保護於刑事事務之警方及司法合作框架下處理之個人資料制定理事會框架決定第 2008/977/JHA 號（官方公報 L 類第 350 期，2008 年 12 月 30 日，第 60 頁）。

scope of application of that Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(6) 理事會框架決定第 2008/977/JHA 號 4 適用於刑事事務之司法合作及警方合作領域。框架決定之適用範圍限於會員國間傳輸或開放之個人資料處理。

(7) Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(7) 確保一致且高度之個人資料保護，及促進會員國之主管機關間個人資料交換，對於確保有效之刑事事務之司法合作及警方合作是重要的。為達該目標，有關主管機關就預防、調查、偵查及追訴刑事犯罪或執行刑罰目的所為之個人資料處理，包括為維護及預防此等資料對歐盟內公共安全及個人資料自由流通造成之威脅，個人權利及自由保護之程度在所有會員國內應相等。歐盟全境內有效之個人資料保護需要強化資料主體之權利，並強化個人資料處理者與具監督及確保會員國內個人資料保護規

則遵循之同等權力者之義務。

(8) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural person s with regard to the processing of personal data and the rules relating to the free movement of personal data.

(8) 歐洲聯盟運作條約第 16 條第 2 項要求歐洲議會及歐盟理事會設立關於個人資料處理及確保歐盟內個人資料自由流通下有關保護個人之一般規則。

(9) On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council [5] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(9) 在該基礎下，歐洲議會及歐盟理事會之歐盟規則第 2016/679 號 5 設立了關於個人資料處理及確保歐盟內個人資料自由流通下有關保護個人之一般規則。

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(10) 在關於刑事事務之司法合作及警方合作領域之個人資料保護之

---

[5] 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) (see page 1 of this Official Journal).
歐洲議會及歐盟理事會於 2016 年 4 月 27 日為保護個人有關個人資料處理及自由流通制定歐盟規則第 2016/679 號，並廢止歐盟指令第 95/46/EC 號（一般資料保護規則）（參此官方公報第 1 頁）。

第 21 號聲明，即由通過里斯本條約之跨政府會議列為最終法案之附件，該會議已承認：因刑事事務之司法合作及警方合作領域之特殊性質，依歐洲聯盟運作條約第 16 條於該等領域之個人資料保護及個人資料自由流通有其特別規定之必要。

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities.

(11) 因此，在該等領域，關於主管機關基於預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的而為個人資料處理之個人資料保護，應由訂有相關特別規定之指令來處理，包括對公共安全之威脅的防護措施或預防，並應注重該等活動之特殊性質。

Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies.

該等主管機關不僅可能包括司法機關、警察或其他執法機關，亦可能包括任何會員國為本指令之目的所立法委託行使公權力之機構或實體。當該等機構或實體處理個人資料係為了本指令之目的以外之其他目的時，歐盟規則第 2016/679 號有其適用。

Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to

which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.
因此，當一機構或實體為其他目的蒐集個人資料，並進一步處理該等個人資料以遵守其法律上義務時，歐盟規則第 2016/679 號在該等情形有其適用。例如，為了調查、偵查或追訴刑事犯罪，金融機構持有其等曾處理之特定個人資料，並在特定情形下依據會員國法僅提供該等個人資料予會員國之主管機關。

A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.
代主管機關在本指令之範圍內處理個人資料之機構或實體，應受契約或其他法律以及適用於本指令所規範處理者之條款的拘束，惟就本指令範圍以外之處理者對於個人資料處理，歐盟規則第 2016/679 號之適用不受影響。

(12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots.

(12) 由警察或其他執法機關執行之活動係主要集中在預防、調查、偵查或追訴刑事犯罪，包括事先並不知情該事件是否為刑事犯罪之警察活動。該等活動亦可包括公務機關強制手段之施行，

例如在示威活動、大型體育活動或暴動之警察活動。

They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.

此亦應包括當有必要保護或預防對受法律保護之社會公共安全及基本權利之威脅，且該等威脅可能導致刑事犯罪時，警察或其他執法機關被賦予任務維持法律或秩序之情形。會員國得委託主管機關為非必然為上開預防、調查、偵查及追訴刑事犯罪目的之其他任務，包括保護或預防對於公共安全之威脅，以使為該等其他目的之個人資料處理——只要其尚在歐盟法之範圍內——得含括於歐盟規則第 2016/679 號之範圍內。

(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the 'Court of Justice').

(13) 本指令中刑事犯罪之意義，應如同歐盟法院之闡釋，為歐盟法下之獨立概念。

(14) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out

activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.

(14) 因本指令不應適用於歐盟法涵蓋範圍以外之活動過程中之個人資料處理，故關於國家安全之活動、局處或單位處理國家安全問題之活動，以及會員國實行涵蓋於歐盟條約（即 TEU）第五篇第二章內之活動時之個人資料處理，不應被認為係本指令涵蓋範圍內之活動。

(15) In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(15) 為確保在歐盟境內透過法律上可執行之權利對個人有相同程度之保護，並避免歧異性阻礙了主管機關間個人資料之流通，本指令應為預防、調查、偵查或追訴刑事犯罪或執行刑罰之目的（包括保護或預防對於公共安全之威脅）所進行個人資料處理之保護及自由流通提供協調一致之規範。

The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

會員國法之相似性不應造成會員國提供之個人資料保護之減少，

相反地應試圖確保在歐盟境內得受高程度之保護。關於主管機關處理個人資料，會員國不應被禁止提供比本指令所建立者更高之保護機制以保障資料主體之權利及自由。

(16) This Directive is without prejudice to the principle of public access to official documents. Under Regulation (EU) 2016/679 personal data in official documents held by a public authority or a public or private body for the performance of a task carried out in the public interest may be disclosed by that authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

(16) 本指令不妨害公眾取得政府文件之原則。在歐盟規則第2016/679號下，公務機關、公家或私人機構為公共利益執行職務而持有之政府文件可能會被該等機關或機構依據其等所應遵循之歐盟法或會員國法而揭露，以調和公眾取得政府文件及個人資料保護之權利。

(17) The protection afforded by this Directive should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(17) 有關個人資料之處理，本指令所提供之保護應適用於個人，而不問其國籍或住居所。

(18) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Directive.

(18) 為防止產生規避之嚴重風險，當事人之保護應屬技術中立，且不應依賴於已使用之技術。如檔案系統中已包含或旨在包含個人資料者，當事人之保護均有適用，而不問其係透過自動化及手動化方式處理之個人資料。未依照特定標準建構之檔案或檔卷及其等封面則不在本指令之適用範圍內。

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council[6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in Regulation (EU) 2016/679.

(19) 歐洲議會及歐盟理事會 6 所訂定歐盟規則第 45/2001 號適用於歐盟當局、機構、辦事處及局處所為之個人資料處理。歐盟規則第 45/2001 號及其他涉及個人資料處理之歐盟法案應依歐盟規則第 2016/679 號所建立之原則與規定加以調整修正。

(20) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

(20) 本指令不阻礙會員國在其有關法院或其他司法機關對個人資料處理之刑事程序規範中予以具體化規範資料處理活動及處理程

---

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
歐洲議會及歐盟理事會於 2000 年 12 月 18 日為保護個人有關共同體組織及機構處理個人資料及自由流通制定之歐盟規則第 45/2001 號（官方公報 L 類第 8 期，2001 年 12 月 1 日，第 1 頁）。

序，尤其是法院判決或與刑事程序有關之紀錄中所包含之個人資料。

(21) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

(21) 資料保護原則應適用於任何有關識別或得識別個人之資訊。為決定個人是否得識別，應考量無論是控管者或其他人得直接或間接識別出個人之所有合理、可能、得使用之手段，例如挑選。為確定手段是否合理、可能、得使用以識別個人，應考量所有客觀因素，例如識別所需時間之成本及長度，考慮當時可及之處理技術與科技發展。因此，資料保護支援不應適用於匿名資料，即與受識別或得識別之個人無關之資訊，亦不適用於以匿名方式使資料主體不再為可識別之個人資料。

(22) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets

should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

(22) 執行公務而取得依法定義務所揭露個人資料之公務機關，諸如稅務機關及海關、金融調查單位、獨立行政機關或負責規範及監管證券市場之金融市場主管機關，如其接收個人資料係為公眾利益所必要而進行特定詢問者，該公務機關非屬歐盟法或會員國法所定之資料接收者。公務機關要求揭露應以書面、附理由且偶然為之，且不得通用於整個檔案系統或與其他檔案系統相聯通。公務機關處理個人資料應依照其處理之目的，遵守可適用之資料保護規則。

(23) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person and which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(23) 基因資料係指經由當事人生物樣本分析後所涉及該當事人遺傳性或突變性之基因特徵之個人資料，特別是染色體、去氧核糖

核酸（DNA）或核糖核酸（RNA）分析或從其他元素可獲得相同資料之分析。考慮到基因資訊之複雜性與敏感性，有由控管者為各種目的而誤用與重複使用之極大風險。任何基於基因特徵之歧視原則上應受禁止。

(24) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council[7] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(24) 關於健康之個人資料應包括資料主體所揭露關於過去、現在或未來生理或心理健康狀態而與該資料主體健康情況有關之全部資料。其中包括在為當事人登記之過程中或為其提供依照歐洲議會及歐盟理事會[7]所定第 2011/24/EU 號指令定義之醫療照顧服務中所蒐集之資訊；為醫療目的特別配予當事人而用以識別該人之號碼、標誌或獨特標識；對身體部位或組成物質（包括

[7] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
歐洲議會及歐盟理事會於 2011 年 3 月 9 日就跨境醫療保健之病患權利制定之歐盟指令第 2011/24/EU 號（官方公報 L 類第 88 期，2011 年 4 月 4 日，第 45 頁）。

基因資料或生物樣本）進行測試或檢驗所得到之資訊；及從醫生或其他醫療專業人員、醫院、醫療裝置或體外診斷測試等獨立於資料主體以外來源所得之任何資訊，例如：疾病、殘疾、患病風險、病史、臨床治療或該資料主體之生理狀態或醫學狀態。

(25) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA[8] and Council Decision 2007/533/JHA[9].

(25) 所有會員國皆隸屬於國際刑警組織。為完成其任務，國際刑警組織會接收、儲存並計算個人資料以協助主管機關預防並打擊國際犯罪。因此，透過提升有效的個人資料交換並同時確保尊重有關個人資料自動化處理之基本權與自由，強化歐盟與國際刑警組織之合作乃是適當的。當個人資料從歐盟移轉至國際刑

---

[8] Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).
2005年1月24日就制定之理事會共同立場第2005/69/JHA號（官方公報L類第27期，2005年1月29日，第61頁）。

[9] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).
2007年6月12日就第二代申根資訊系統（SIS II）之建構、運作及使用制定之理事會決定第2007/533/JHA號（官方公報L類第205期，2011年8月7日，第63頁）。

警組織及有代表於國際刑警組織的國家，本指令，尤其是國際移轉之條文，應有其適用。本指令不應損及理事會之共同立場第 2005/69/JHA 號[8] 及理事會決定第 2007/533/JHA 號[9] 之特別規定。

(26) Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary,

time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(26) 與當事人有關之任何個人資料處理必須合法、公正且透明，且僅得基於法律設定之特定目的為處理。此不當然使執法機關不得實行如秘密調查或錄影監控之活動。若此等活動為法律規定且屬在民主社會中所必要且適度之措施，並適當考慮當事人之正當利益，其得基於預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的而進行，包括為維護及預防對公共安全造成威脅。公平處理之資料保護原則係憲章第 47 條及歐洲人權公約第 6 條所定義之公平審判權下的重要概念。當事人應受告知關於個人資料處理之風險、規則、保護措施及權利，以及關於處理之權利如何行使。尤其，資料處理之特定目的應明確且正當，並於蒐集個人資料時即確定。個人資料應充分且與其受處理之目的相關。此尤應確保蒐集之個人資料不過量且保存不得超過處理目的所必要之時間。個人資料應僅於處理之目的無法以其他手段合理滿足時受處理。為確保保存不超過處理目的所必要之時間，刪除或定期審查之時間限制應由控管者建立。基於公共利益、科學、統計或歷史用途之較長期資料保存，會員國應為其擬定適當之個人資料保護措施。

(27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.

(27) 為了預防、調查及追訴刑事犯罪，主管機關有必要跨越原脈絡而處理因預防、調查、偵查或追訴特定刑事犯罪蒐集而來個人

資料，以發展對於犯罪活動之了解，並連結不同犯罪間之偵查。

(28) In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(28) 為了維持有關處理之安全並預防處理違反本指令，個人資料應以確保適當之安全及機密程度之態度處理，包括預防未授權之接近使用或利用個人資料，亦應以考慮有關欲保護之個人資料的風險及本質之現有狀況、技術與執行費用之態度處理。

(29) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.

(29) 個人資料應在本指令之範圍內為特定、明確且正當之目的予以蒐集，且不應以與預防、調查、偵查及追訴刑事犯罪或執行刑罰（包括為維護及預防對公共安全造成威脅）等不相容之目的處理。若個人資料由相同或其他控管者基於本指令範圍內非原本蒐集之目的處理，此等處理應於依可適用之法規授權及對該

目的必要且適當之條件下受允許。

(30) The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(30) 資料正確之原則於考量有關處理之本質與目的時應適用。尤其於司法程序，包含個人資料之陳述係基於當事人之主觀感知，且並非總是可驗證的。因此，資料正確之要求不應與陳述之正確有關，而僅與已作成之特定陳述之事實有關。

(31) It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.

(31) 有關資料主體不同分類之個人資料處理，係刑事事務之司法合作及警方合作領域之個人資料處理所固有的。因此，當清楚的區別係可適用且有可能時，應於資料主體之不同分類間區別，例如：嫌疑犯；受判決有刑事犯罪者；受害人與其他方如目擊者；處理相關資訊或聯絡人之人；或嫌疑犯或刑事罪犯之協助者。

誠如歐盟法院及歐洲人權法院判例法分別之解釋，此不應使憲章及歐洲人權公約所保證之無罪推定原則無法適用。

(32) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure the protection of natural persons, the accuracy, completeness or the extent to which the personal data are up to date and the reliability of the personal data transmitted or made available, the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(32) 主管機關應確保不正確、不完整或不合時宜之個人資料不受傳輸或開放。為了確保當事人之保護，正確性、完整性或個人資料更新之程度以及個人資料傳輸或開放之可信度，主管機關應在可能之範圍內於所有個人資料之傳輸增加必要之資訊。

(33) Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(33) 當本指令提及會員國法、法律基礎或立法措施者，並不必然要求國會之立法，亦不影響對相關會員國之憲政秩序追求之要求。然而，此等會員國法、法律基礎或立法措施應清楚且簡潔，且

其適用應對主體而言可預見，如歐盟法院及歐洲人權法院判例法之要求一般。本指令範圍內有關個人資料處理之會員國法，至少應特定客體、欲處理之個人資料、處理之目的、以及維護個人資料之完整性與機密性之程序及其銷毀程序，並因此提供了避免濫用與專斷之充分保證。

(34) The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority. Where personal data were initially collected by a competent authority for one of the purposes of this Directive, Regulation (EU) 2016/679 should apply to the processing of those data for purposes other than the purposes of this Directive where such processing is authorised by Union or Member State law. In particular, the rules of Regulation (EU) 2016/679 should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, Regulation (EU) 2016/679 should apply. While implementing this

Directive, Member States should also be able to further specify the application of the rules of Regulation (EU) 2016/679, subject to the conditions set out therein.

(34) 主管機關基於預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的，包括為維護及預防對公共安全造成威脅，應包含以該等目的而就個人資料或系列個人資料處理之任何活動或任何系列活動，不問是自動化方式或其他，例如蒐集、紀錄、組織、架構、儲存、改變或調整、撤回、諮詢、使用、校準或合併、處理之限制、刪除或銷毀。尤其，本指令之規則應適用於基於本指令之目的而以非本指令之主體為接收者的個人資料傳輸。該等接收者應包括自然人或法人、公務機關、機構或其他任何由主管機關合法揭露個人資料之主體。當個人資料由主管機關基於本指令之目的之一有意識地蒐集時，歐盟規則第 2016/679 號應適用於經歐盟或會員國法授權而基於本指令以外目的對該等資料之處理。由主管機關合法揭露個人資料予非主管機關之接收者或非本指令意旨下以主管機關身分接收者，就該等接收者所為之個人資料處理，歐盟規則第 2016/679 號應有適用。於執行本指令時，會員國亦應得進一步特定歐盟規則第 2016/679 號之規則的適用，但須符合其中所列之條件。

(35) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent

authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

(35) 為求合法，本指令下之個人資料處理應為主管機關基於歐盟或會員國法為達成預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的，包括為維護及預防對公共安全造成威脅，而為公益執行職務所必要者。該等活動應包含對資料主體重要利益之保護。法律制度性地賦予主管機關預防、調查、偵查及追訴刑事犯罪之職務執行使主管機關得請求或命令其他個人遵循其請求。於此情形，如歐盟規則 2016/679 所定義之資料主體之同意，不應提供主管機關處理個人資料之合法基礎。當資料主體被要求遵循法律義務時，資料主體並沒有真摯而自由之選擇，因此資料主體之反應不得被視為自由地基於其意願給予表示。此不應排除會員國得依法使資料主體得同意其個人資料基於本指令之目的而受處理，如犯罪調查中之 DNA 測試或為執行刑罰以電子標記監控其地點。

(36) Member States should provide that where Union or Member State law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as the use of handling codes, the transmitting competent authority should inform the recipient of such

personal data of those conditions and the requirement to respect them. Such conditions could, for example, include a prohibition against transmitting the personal data further to others, or using them for purposes other than those for which they were transmitted to the recipient, or informing the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority.

(36) 會員國應規定，於傳輸主管機關之歐盟法或會員國法有其適用時所定特別情況下之個人資料處理的特殊條件，例如就處理程式碼之使用時，會員國應規定傳輸主管機關應通知接收者關於該等個人資料之條件及遵守此等條件之要求。此等條件得包括如對進一步傳輸個人資料予他人，或使用該等資料於傳輸予接收者以外之目的，或在限制知悉權之情況下未得到傳輸主管機關同意前即通知資料主體之禁止。

Those obligations should also apply to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should ensure that the transmitting competent authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar data transmissions within the Member State of that competent authority.

該等義務亦應適用於傳輸主管機關對位於第三國或國際組織之接收者的移轉。會員國應確保傳輸主管機關不將該等條件適用於其他會員國之接收者或並未在該主管機關所屬會員國中適用類似之資料傳輸而依照歐洲聯盟運作條約第五篇第四章、第五章設立之局處、辦事處及機構。

(37) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the

fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races.

(37) 依其本質對基本權及自由特別敏感之個人資料，因其處理過程中可能對於基本權及自由造成顯著風險，故值得受到特別保護。該等個人資料應包括顯示出種族或人種之個人資料，但本指令使用「種族」乙詞並不代表歐盟承認旨於區別個別種族存在之理論。

Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.

該等個人資料不得處理，除非其處理係依照法律所規定對資料主體權利及自由之適當保護措施，且係法律所授權之情形；非該等法律已授權，但該處理對於保護資料主體或他人之重要利益為必要；或該處理係關於由資料主體明顯已自行公開之資料。

Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground

for processing such sensitive personal data by competent authorities.
對於資料主體之權利及自由適當之保護措施得包括僅蒐集與該個人之其他資料相關之資料的可能性，確保資料被適當地蒐集的可能性，對於主管機關職員接近使用該資料更嚴格之規範，以及對傳輸該等資料之禁止。當資料主體明確同意特別會對其造成侵擾之資料處理，則該等資料之處理亦應為法律所准許。然而，資料主體之同意本身不應構成主管機關處理該等敏感個人資料之合法依據。

(38) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

(38) 資料主體應有權不受僅以自動化處理來評估其個人特徵且對其產生不利之法律效果或造成重大影響之決定的拘束。在任何情況下，該等處理應有適當之保護措施，包括對資料主體為特定資訊之提供以及獲得人為干預之權利，特別是表達其意見、獲得依上開評估後做成決定之解釋，或挑戰該決定之權利。基於與基本權利及自由有關，性質上特別敏感之個人資料而造成對個人歧視之建檔，在憲章第 21 條及第 52 條所規定之條件下應被禁止。

(39) In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children.

(39) 為使資料主體得行使其權利，任何給予資料主體之資訊應易於接近使用，包括在控管者之網站上，且應易於理解、使用清楚且淺白之語言。該等資訊應適於如兒童等易受傷害之個人的需求。

(40) Modalities should be provided for facilitating the exercise of the data subject's rights under the provisions adopted pursuant to this Directive, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and restriction of processing. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with this Directive.

(40) 為利於資料主體行使依照本指令採用之規定下的權利，應提供不同之免費管道，包括請求之機制及（如有可能）獲得之機制，尤其是接近並更正或刪除個人資料及限制該處理。控管者有義務回應資料主體之要求，不得無故遲延，除非控管者適用依據本指令對於資料主體權利之限制。

Moreover, if requests are manifestly unfounded or excessive, such as where the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller should be able to charge a reasonable fee or refuse to act on the request.

此外，若所為之要求明顯無事實根據或過度，例如當資料主體不合理且重複不斷地要求資訊，或當資料主體濫用其接收資訊

之權利（例如提出要求時提供錯誤或誤導之資訊）時，控管者應得收取合理之費用或拒絕回應該要求。

(41) Where the controller requests the provision of additional information necessary to confirm the identity of the data subject, that information should be processed only for that specific purpose and should not be stored for longer than needed for that purpose.

(41) 當控管者要求提供確認資料主體之身分所必須之額外資訊，該資訊應僅得為該特別目的而被處理，且其儲存不應久於對該目的之需求。

(42) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority.

(42) 應使資料主體至少得獲取以下資訊：控管者之身分、處理活動之存在、處理之目的、提出申訴之權利，及向控管者要求取得並更正或刪除個人資料及限制該處理之權利的存在。此可於主管機關之網站上提供。

In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

此外，在特定案件且為確保資料主體得行使其權利，只要該等進一步之資訊對於確保該處理對資料主體之公正性係有必要，且將特殊情況下之資料處理納入考量時，應通知資料主體該處理之法律依據，以及該資料將被儲存之時間長短。

(43) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries.

(43) 資料主體應有權接近使用其所受蒐集之個人資料，並得容易地、於合理之時間間隔內行使接近使用權，以知悉並核實該處理之合法性。因此，各資料主體應有權知悉並溝通關於個人資料受處理之目的、受處理之期間及個人資料之接收者（包括位於第三國者）。

Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

當該等溝通包括關於個人資料來源之資訊時，該資訊不應揭露個人之身分，尤其是機密之出處。為使資料主體得以行使本指令賦予其等之權利，應使該資料主體持有關於該等資料完整摘要之明瞭表格，亦即一個能使資料主體意識到該等資料並確認其為正確且係依照本指令而為處理之表格。該摘要得以正在進行處理之個人資料副本之形式提供。

(44) Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(44) 會員國得採取延緩、限制或刪除關於資料主體之資訊，或全部或部分限制接近使用其等之個人資料的立法措施，只要該措施在民主社會下符合必要性及比例性，並應注意基本權及相關個人之正當利益，以避免阻礙官方或依法之詢問、調查或程序，並避免妨礙對刑事犯罪之預防、調查、偵查及追訴或刑罰之執行，以保護公共安全或國家安全，或保護他人之權利及自由。控管者應透過對各個事件具體且個別之檢查，以評估接近使用之權利是否需部分或全部被限制。

(45) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(45) 任何對接近使用之拒絕或限制原則上應對資料主體以書面為之，並包括該決定所依據之事實上及法律上理由。

(46) Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights

respectively, and in particular respect the essence of those rights and freedoms.

(46) 任何對資料主體權利之限制必須遵守憲章以及歐洲人權公約（即ECHR），並個別依照歐盟法院及歐洲人權法院判例之闡釋，且特別尊重此等權利及自由之本質。

(47) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence.

(47) 當事人應有權利，尤其是當該資料與事實有關時，令有關於其個人之不正確個人資料為更正，以及有權利對違反本指令之資料處理為刪除。然而，更正之權利不應影響如證人證詞之內容。於當事人質疑個人資料之正確性且其正確性或不正確性不能被確認時，或當個人資料須為證據之目的被留存時，當事人亦應有限制資料處理之權利。

In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is

restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

尤其，若在特殊情況下有合理理由相信資料之刪除會影響資料主體之正當利益時，則應不為刪除而係限制對資料之處理。在該等情況下，被限制之資料應僅得為其不得刪除之目的而被處理。限制個人資料處理之方法包括但不限於將所選之資料移至另一個處理系統，例如存檔目的，或使所選之資料無法被取得。在自動歸檔系統對處理之限制原則上應由科技方式來確保。該等對個人資料之更正或刪除或對資料處理之限制應向接收者、資料揭露之對象及產生不正確資料之主管機關傳達。控管者亦應避免該等資料之進一步傳播。

(48) Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(48) 當控管者否認資料主體有知悉、接近使用或更正或刪除個人資料或限制資料處理之權利時，資料主體應有權要求該國監管機關核實該處理之合法性。資料主體應被告知有該等權利。當監管機關代資料主體為行為時，資料主體至少應被監管機關告知

監管機關已為之所有必要之核實或檢驗。監管機關亦應告知資料主體有尋求司法救濟之權利。

(49) Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.

(49) 當個人資料在刑事案件之刑事調查及法院程序之過程中被處理時，會員國得規定知悉、接近使用或更正或刪除個人資料或限制資料處理權利之行使應依照各國對司法程序之規範。

(50) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.

(50) 就任何由控管者所實行或代表控管者實行之個人資料處理，控管者之責任與義務應被建立。尤其，控管者應有義務實行適當且有效之手段，並應證明處理活動係依照本指令之規定而為之。該等手段應考量處理之性質、範圍、內容及目的，以及對個人權利及自由之風險。控管者所使用之手段應包括制定並實行對易受傷害之個人（如兒童）個人資料之處置的特定保護措施。

(51) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which

could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(51) 當事人之權利及自由所受之諸多可能且嚴重之風險，可能起因自處理個人資料，並造成身體上、物質上、或非物質上之損害，尤其是於下述情形時：當處理可能造成歧視、身分盜用或詐欺、金融損失、名譽損害、受職業性秘密保護之個人資料喪失機密性、假名化未授權撤銷、或其他任何顯著之經濟性或社會性之不利益時；當資料主體之權利或自由可能受到剝奪或被排除在自己之個人資料控制權之外時；當個人資料處理涉及揭露種族或人種、政治意見、宗教或哲學信仰、貿易聯盟會員、以及基因資料之處理、有關健康之資料或有關性生活或前科及犯罪或

相關保安措施之資料時；當個人特徵受到評估，尤其是為了建檔或使用個人檔案，分析或預測有關工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、地點或動向等個人特徵時；當處理易受傷害之個人（尤其是兒童）之個人資料時；或當該處理會牽涉大量個人資料並影響大量資料主體時。

(52) The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(52) 權利與自由所受風險之嚴重性及可能性應參考資料處理之本質、範圍、過程與目的定之。風險應在客觀評鑑基礎上被評估，並藉以確定資料處理活動是否有風險或有高度風險。高度風險係對資料主體之權利與自由造成侵害之特殊風險。

(53) The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures should not depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter alia, of the use of pseudonymisation, as early as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data

within the area of freedom, security and justice.

(53) 關於個人資料處理之權利及自由保護必須採取適當之科技化且有組織的措施，以確保符合本指令之要求。該等措施之執行不應僅倚賴經濟考量。為了得以證明符合本指令，控管者應採取符合特別是設計與預設資料保護原則之內部規則與執行措施。當控管者依照本指令實行資料保護影響評估，結果應於發展該等措施與程序時受到考量。措施得包括但不限於盡早進行假名化之使用。為本指令之目的使用假名化，得作為促進尤其是自由、安全與正義領域內個人資料自由流通之工具。

(54) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities set out in this Directive, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(54) 資料主體之權利與自由保護與控管者及處理者之責任與義務（此也均與監管機關之監控與其手段有關）應依本指令予以明確分配，包括於控管者與其他控管者共同決定資料處理之目的與手段時，或是由控管者之代表進行處理活動時。

(55) The carrying-out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(55) 處理者就處理之執行應受到法令控管，包括將處理者結合至控管者，並規定處理者僅得依控管者之指示行動之契約。處理者應將設計及預設之資料保護原則納入考量。

(56) In order to demonstrate compliance with this Directive, the controller

or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(56) 為證明遵循本指令，控管者或處理者應依其職責保留處理活動之紀錄。各控管者及處理者應有義務配合監管機關並做成前開紀錄，並依要求提供之，使處理活動受監控。以非自動處理系統處理個人資料之控管者或處理者應有適當而有效率之方法證明處理之合法性、啟用自我監測以及確保資料完整與資料安全性，例如日誌或其他形式之紀錄。

(57) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(57) 日誌應至少為如蒐集、調整、諮詢、揭露等自動處理系統之活動保存，包括移轉、合併或刪除。諮詢或揭露個人資料者之識別應被記錄，且從該識別中，應得確定處理活動之理由。日誌應僅能使用於驗證處理之合法性、自我監控以確保資料完整性

與資料安全性、以及刑事程序。自我監控亦包括主管機關之內部管理程序。

(58) A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.

(58) 於處理活動基於其本質、範圍或目的，尤其是包括旨在確保個人資料保護及符合本指令之措施、維護與機制，可能造成對資料主體權利及自由之高風險時，控管者應實行資料保護影響評估。影響評估應包括相關系統與處理活動之處理，惟不包括個案。

(59) In order to ensure effective protection of the rights and freedoms of data subjects, the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(59) 為了確保有效保護資料主體之權利與自由，控管者或處理者應徵詢監管機關，且在某些案件應先於處理。

(60) In order to maintain security and to prevent processing that infringes this Directive, the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure

of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage. The controller and processor should ensure that the processing of personal data is not carried out by unauthorised persons.

(60) 為維持安全性與預防資料處理違反本指令，控管者或處理者應評估與處理相關之風險，並執行相關措施以降低風險，例如加密。該等措施應確保適當之安全程度，包括機密性，且考慮到有關欲保護之個人資料的風險及本質之現有技術狀況與執行費用。於衡量資料安全風險時，應考慮因個人資料處理所造成之風險，例如意外或非法破壞、遺失、變更、未獲授權之揭露或接近使用、個人資料之傳輸、儲存或其他可能特別引起身體上、物質上或非物質上之損害。控管者及處理者應確保個人資料之處理不會由未獲授權者實行。

(61) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for

the delay should accompany the notification and information may be provided in phases without undue further delay.

(61) 若未受到適當且及時之處理，個人資料之侵害可能造成當事人之身體上、物質上或非物質上損害，例如喪失對其個人資料之控制或對其權利之限制、歧視、身分盜用或詐欺、金融損失、假名化未授權撤銷、名譽損害、受職業性秘密保護之個人資料喪失機密性、或其他任何對於所涉當事人之顯著經濟性或社會性之不利益。因此，一旦控管者發現個人資料侵害已然發生，即應向監管機關通報，不得無故遲延，且若可能，應於發現後 72 小時內通報，但控管者得證明依照歸責原則該個人資料之侵害不可能造成當事人之權利與自由的風險者，不在此限。當該通知無法於 72 小時內到達時，遲延之原因應與通知一併提供，且不得有更進一步無故遲延。

(62) Natural persons should be informed without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities.

(62) 為了使當事人得採取必要之預警，當個人資料受侵害可能造成當事人權利及自由之高風險時，當事人應受通知，且不得無故遲延。溝通應描述個人資料侵害之本質，並包括給予當事人有關減低可能之負面影響的建議。對資料主體之溝通應於合理範圍內盡快做成，與監管機關密切合作，並尊重其或其他相關機關提供之指引。

For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

例如，降低損害之立即風險的需求可能需要對資料主體之即時溝通，而對繼續性或類似資料侵害實行適當措施之需求則得正當化較長之溝通時間。於避免妨礙官方或法律詢問、調查、或程序，避免妨礙預防、調查、偵查及追訴刑事犯罪或執行刑罰，保護公共利益、保護國家安全或保護他人之權利及自由無法由延遲或限制對相關當事人之溝通而達成時，該等溝通於例外之情形得省略。

(63) The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller.

His or her task could be carried out on a part-time or full-time basis.

(63) 除非會員國決定於行使其司法權能時排除法院及其他獨立司法機關，控管者應指定一人輔助其監控內部遵循依本指令制定之規定。該人得為控管者既有之員工，曾受過資料保護法之特別訓練並為獲取該領域之專業知識而實作。專業知識所必要之程度尤其應根據實行之資料保護及控管者處理資料所需之保護決定。其任務得以兼職或全職實行。

A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.

考量控管者之組織架構與規模，資料保護員得由多位控管者共同指定，例如於中央單位共享資源之情形。該人亦可受指定至相關控管者之結構中的不同職位。該人應透過通知及建議其有關資料保護義務之遵循，協助控管者及僱員處理個人資料。此種資料保護員應以符合會員國法之獨立態度與職位執行其職責與任務。

(64) Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this

Directive.

(64) 會員國應確保至第三國或國際組織之移轉僅發生於預防、調查、偵查及追訴刑事犯罪或執行刑罰之目的有必要時，包括為維護及預防此等資料對歐盟內公共安全及個人資料自由流通造成之威脅，且於第三國或國際組織之控管者為本指令意義下之主管機關。

A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply.

除非處理者受到明確指示代控管者進行移轉，移轉應僅得由主管機關以控管者身分執行。此種移轉可能發生於執委會決定系爭第三國或國際組織確保充足程度之保護時、提供適當保護措施時、以及適用特殊情形之例外時。

Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.

當個人資料從歐盟移轉至第三國或國際組織之控管者、處理者或其他接收者時，歐盟本指令所提供之當事人保護程度不得被破壞，包括個人資料從第三國或國際組織至同一或其他國家或國際組織之控管者或處理者的進一步移轉。

(65) Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in

principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law-enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations.

(65) 當個人資料從一會員國移轉至第三國或國際組織，原則上該移轉應僅得於資料獲得之會員國授權後進行。有效率執法合作之利益要求當性質上對會員國或第三國之公共安全或對會員國之重要利益之威脅非常立即，且及時獲得授權不可能時，主管機關應得於未受該等事先授權之情形下移轉相關個人資料予第三國或相關國際組織。會員國應規定任何有關移轉之特定條件應傳達予第三國或國際組織。

Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific

conditions. Such specific conditions can be described, for example, in handling codes.

進一步的個人資料移轉應獲得執行原始移轉之主管機關事先授權之控制。決定授權進一步移轉之請求時，執行原始移轉之主管機關應適當考量所有相關因素，包括刑事犯罪之嚴重性、資料原始移轉之具體條件與目的、刑罰執行之本質與條件、以及進一步移轉轉入之第三國或國際組織對個人資料保護之程度。執行原始移轉之主管機關亦應得以特定條件控制進一步移轉。該等特定條件得以如處理準則之方式描述。

(66) The Commission should be able to decide with effect for the entire Union that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer.

(66) 執委會得做成影響全歐盟之決定，認定第三國、第三國內之領域或特定部門，或國際組織已提供充足程度之資料保護，並因此就第三國或國際組織被認為已提供該保護程度乙事在整個歐盟提供了法明確性和一致性。於該等情形，個人資料移轉至第三國或國際組織應得於不需要獲得進一步授權之情形下進行，除非自其獲取資料之會員國必須給予移轉之授權。

(67) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular

third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security, as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(67) 依循歐盟所創立之基本價值，尤其是人權之保護，執委會在其衡量第三國或第三國內之領域或特定部門時，應考量特定第三國如何遵守法治、接近使用司法、以及國際人權規範和標準及其普通法與部門法，包括涉及公共安全、防禦與國家安全與公共秩序及刑法之立法。對第三國內之領域或特定部門作成有提供充足保護之決定應考量明確與具體之標準，例如特定處理活動及第三國可適用之法律標準與立法之範圍。第三國應提供保證，以確保基本上等同於歐盟所保障之充足程度保護，特別是當個人資料處理在單一或數個特定部門時。尤其，第三國應確保有效而獨立之資料保護監督機制，且應提供合作機制予會員國資料保護機關，且應提供資料保護主體有效且可實現的權利與有效的行政與司法救濟。

(68) Apart from the international commitments the third country or

international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board established by Regulation (EU) 2016/679 (the 'Board') when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679.

(68) 除了第三國或國際組織已加入之國際協約，執委會應考量第三國或國際組織於多邊或區域體系之義務，尤其是涉及個人資料保護及該等義務之履行。尤其，應考量第三國加入歐洲理事會 1981 年 1 月 28 日關於自動化個人資料處理之個人保護公約及其附加議定書。於衡量第三國或國際組織之保護程度時，執委會應向歐盟規則第 2016/679 號設立之歐洲資料保護委員會（下稱「委員會」）諮詢。執委會亦應考量其依歐盟規則第 2016/679 號第 45 條作成之任何相關充足保護之決定。

(69) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be undertaken in consultation with the third country or international organisation in question and should take into account all relevant

developments in the third country or international organisation.

(69) 執委會應觀察審視第三國、第三國境內之領域或特定部門、或國際組織保護程度之決定的運作。就有提供充足保護之決定，執委會應提供定期檢驗其運作之機制。該定期檢驗應在諮詢有關之第三國或國際組織下進行，且考量所有相關第三國或國際組織之發展。

(70) The Commission should also be able to recognise that a third country, a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements in this Directive relating to transfers subject to appropriate safeguards and derogations for specific situations are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(70) 執委會可能認定第三國、第三國內之領域或特定部門、或國際組織不再達到充足程度之資料保護。因此，向該第三國或國際組織之個人資料移轉應被禁止，但完成本指令關於移轉所定適當保護措施之要件被滿足，及存在特定情況之例外者，不在此限。在該情況，該規範應由執委會及該第三國或國際組織間訂定。執委會應於適當時間內通知第三國或國際組織其理由，並進入協商程序以救濟該情形。

(71) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that

appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress.

(71) 非基於有提供充足保護決定之移轉，僅得於已以確保個人資料保障而具法律拘束力之文書提供適當保護措施時，或於控管者已評鑑所有資料移轉之相關環境、且在該評鑑之基礎上認為有關個人資料保護之適當保護措施存在時，受到允許。例如，該等具法律拘束力之文件可能是如由會員國締結並於其法秩序執行、並得由資料主體強制執行之具法律拘束力的雙邊協約，確保資料保護要求之遵循及資料主體之權利，包括獲得有效的行政與司法救濟之權利。

The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

控管者於執行所有有關資料移轉之環境評鑑時應將歐洲刑警組

織或歐洲司法合作組織與第三國所締結，允許個人資料交換之合作條約納入考量。控管者應亦考量個人資料移轉須遵守機密義務與明確性原則，以確保資料不會受到因移轉所為目的以外之其他目的處理。此外，控管者應考量個人資料不會被用於要求、宣告或執行死刑或任何形式之殘忍及不人道之待遇。縱於該等條件可被評價為允許資料移轉之適當保護措施時，控管者應仍得要求額外之保護措施。

(72) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(72) 當不存在提供充足保護之決定或適當保護措施時，移轉或各類型之移轉僅得於特定情形發生，如有必要保障資料主體或他人之重要利益，或保護會員國法移轉個人資料時所提供資料主體之正當利益；為預防對會員國或第三國公共安全立即且嚴重之威脅;於個案中為預防、調查、偵查及追訴刑事犯罪或執行刑罰，

包括為維護及預防此等資料對歐盟內公共安全及個人資料自由流通造成之威脅；或於個案中為建立、實行或防禦法律主張時。該等例外應被嚴格解釋，不應允許頻繁、大量且結構性之個人資料移轉、或大規模之資料移轉，且應限於嚴格地必要之資料。該等移轉應有紀錄，並應得基於監管機關之要求而進行，以監控移轉之合法性。

(73) Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries.

(73) 會員國之主管機關適用現行與第三國締結之關於刑事事務與警方合作之司法合作雙邊或多邊國際協約，以交換相關資訊使其得實行其依法分派之任務。原則上，此為透過、或至少與第三國之主管機關為本指令之目的合作所進行的，有時甚至並無雙邊或多邊國際協約。然而，於特定個案，一般程序要求接觸第三國之機關可能是無效或不適當的，尤其因為移轉可能不會及時執行，或因為第三國之機關並不重視法治或國際人權規範與標準，因此會員國之主管機關得決定直接移轉個人資料予第三

國設立之接收者。

This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

可能之情形如為了拯救成為刑事犯罪受害者而陷於危險之生命、或為了防止即將發生之犯罪，包括恐怖主義，而有移轉個人資料之緊急需求。即便此種在主管機關與第三國建立之接收者間的移轉僅應於特定個案發生，本指令應提供規範該等情形之條件。該等條文不應被視為現行關於刑事事務與警方合作之司法合作雙邊或多邊國際協約之例外。此外，該等規範應適用本指令之其他規則，尤其是有關處理合法性者及第五章。

(74) Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data

protection supervisory authorities to help them exchange information with their foreign counterparts.

(74) 當個人資料跨境移轉時，會增加當事人行使資料保護權利以保護其免於該等資料非法使用或揭露之風險。同時，監管機關可能會發現其無法對境外之活動追究申訴或進行調查。在跨境之脈絡下其合作之努力可能會受到不充分的預防或救濟權力及不一致之法律機制所阻礙。因此，資料保護監管機關間有需要提升更緊密之合作，以協助其與國外對應之組織交換資訊。

(75) The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. To that end, the supervisory authorities should cooperate with each other and with the Commission.

(75) 會員國設置得獨立執行其完整任務之監管機關，係對當事人有關資料處理保護之重要要素。監管機關應監控依本指令採行之規定的適用，並應致力於全歐盟內之一致適用，以達對當事人有關資料處理之保護。為此，監管機關應互相合作並與執委會合作。

(76) Member States may entrust a supervisory authority already established under Regulation (EU) 2016/679 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(76) 會員國得將應依本指令建立之國家監管機關須實行任務之責任，委託予已依歐盟規則第 2016/679 號建立之監管機關。

(77) Member States should be allowed to establish more than one

supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(77) 會員國應受允許建立一個以上的監管機關以反映其憲法上、組織上以及行政上之結構。各監管機關應獲提供足以有效執行其任務（包括與歐盟其他監管機關互助及合作有關之任務）之金融與人力資源、辦公室與基礎設施。各監管機關應有獨立、公共之年度預算，其得為國家或聯邦預算之一部分。

(78) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that such financial control does not affect their independence.

(78) 監管機關就其財務支出，應受獨立之控制或監督機制約束，但該等財務控制不應影響其等之獨立性。

(79) The general conditions for the member or members of the supervisory authority should be laid down by Member State law and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State based on a proposal from the government or a member of the government, or the parliament or its chamber, or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure.

(79) 關於監管機關成員之一般性規範，應以各會員國法律定之，並應特別規定該等成員係由國會、政府或會員國之元首基於政府、政府官員、國會、國會議院或會員國立法委託之獨立機構之提

案，並依透明之程序而選任。

In order to ensure the independence of the supervisory authority, the member or members should act with integrity, should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. In order to ensure the independence of the supervisory authority, the staff should be chosen by the supervisory authority which may include an intervention by an independent body entrusted by Member State law.

為確保監管機關之獨立性，其成員應依誠信原則為各項行為，避免任何與其職務在性質上不相容之行為，且不應在其任期中從事任何性質上不相容之工作，不問該工作是否受有報酬。為確保監管機關之獨立性，其職員應由監管機關選任，並可能包括會員國立法委託之獨立機構之介入。

(80) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. That exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with Member State law.

(80) 本指令雖亦適用於會員國法院及其他司法機關之活動，惟當個人資料之處理係司法機關行使其司法權時，為確保法院履行其司法任務時得獨立審判，監管機關之權限不應包括該等個人資料之處理。該等豁免應限於法院事件之司法活動，且不應適用於法官依照會員國法可能涉入之其他活動。

Member States should also be able to provide that the competence of the supervisory authority does not cover the processing of personal data of other independent judicial authorities when acting in their

judicial capacity, for example public prosecutor's office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities is always subject to independent supervision in accordance with Article 8(3) of the Charter.

會員國亦應規定監管機關之權限不包括其他獨立司法機關行使其司法權限時之個人資料處理，例如檢察署。在任何情況下，法院及其他獨立司法機關對本指令之規定的遵守皆須受依照憲章第 8 條第 3 項之獨立監督之拘束。

(81) Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

(81) 各監管機關應受理資料主體所提出之申訴，並應調查該事件或傳輸該事件至主管監管機關。監管機關應在受司法審查下就申訴進行調查至對於該特定案件適當之程度。監管機關應在合理期間內通知資料主體就其申訴調查之程序及結果。若該案件需要進一步之調查或須與另一監管機關合作，其間之資訊應提供予資料主體。

(82) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective,

and advisory powers which constitute necessary means to perform their tasks.

(82) 為確保在歐盟境內依照歐盟法院所闡釋之歐洲聯盟運作條約對本指令之遵循及實行為有效、可信及一致之監督，監管機關應在各會員國有相同之任務及有效之權力，包括構成執行其任務之必須手段之調查、糾正及建議之權力。

However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings.

然而，其等之權力不應妨礙對刑事程序之特定規範，包括對刑事犯罪之調查及追訴，或司法之獨立性。對於檢察機關在會員國法所擁有之權力不生影響，監管機關亦應將本指令之違反檢送至司法機關並參與法律程序。

The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down by Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned.

監管機關之權力行使應依歐盟法及會員國法所定適當之程序性保護措施於合理期限內公平、公正為之。尤其，各個措施應具備適當性、必要性及比例性，以確保本指令之遵循、考量個別

案件之情況，並尊重任何人在對其有不利影響之任何個別措施被實施前有請求聽審之權利，且避免對該人造成無謂之花費及過度之不便。

Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

進入處所之調查權應依照會員國法之特別規定為之，例如事先取得司法授權之要求。通過一個具法律拘束力之處分應受作成該處分之監管機關所在會員國的司法審查的拘束。

(83) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(83) 監管機關應互相協助以執行其等之任務並提供互助，以確保對本指令所採納之規範一致之適用及實行。

(84) The Board should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(84) 委員會應致力於本指令在歐盟境內適用之一致性，包括給予執委會建議，並促進全歐盟各監管機關間之合作。

(85) Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses

a complaint or does not act where such action is necessary to protect the rights of the data subject.

(85) 於資料主體認為其依據本指令所採納之規範的權利受到侵害或監管機關對其申訴不予作為、部分或全部不受理或駁回或監管機關應採取作為以保護資料主體之權利卻不作為時，各資料主體應有向個別監管機關提出申訴及依照憲章第 47 條受有效司法救濟之權利。

The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

監管機關應在受司法審查下就申訴進行調查至對於該特定案件適當之程度。主管監管機關應在合理期間內通知資料主體就其申訴調查之程序及結果。若該案件需要進一步之調查或須與另一監管機關合作，其間之資訊應提供予資料主體。

In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

為使申訴之提出能順利進行，各監管機關應採取措施，如提供能以電子格式填具之申訴提交表格，且亦不排除其他溝通管道。

(86) Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints.

(86) 各自然人或法人就監管機關對其作成有法律效果之處分應有權向該管會員國法院尋求有效司法救濟。該處分尤其涉及監管機關調查、糾正及授權之權力行使，以及申訴之不受理或駁回。

However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

然而，該權利並不包含監管機關所採取之不具法律拘束力之其他措施，例如監管機關公告之意見或提出之建議。對監管機關之訴訟應對監管機關設立地之會員國法院提起之，且須依照會員國法之規定進行。此等法院應行使完整之審判權，包括應審理與爭議有關之一切事實上及法律上問題。

(87) Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy.

(87) 當資料主體認為其在本指令下之權利受到侵害，其應有權委任以保護資料主體關於個人資料保護之權利及利益，並依照會員國法所組成之機構來代其向監管機關提起申訴，並行使受司法救濟之權利。

The right of representation of data subjects should be without prejudice to Member State procedural law which may require

mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC[10], before national courts.
為資料主體代理之權利不應損及會員國程序法之規定，即可能要求資料主體在會員國法院須由律師強制代理，如同歐盟理事會第 77/249/EEC 號指令 [10] 之定義。

(88) Any damage which a person may suffer as a result of processing that infringes the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under Member State law. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Directive.

(88) 因違反依本指令通過之規定處理資料所致之一切可能損害，應由控管者或任何其他主管機關依會員國法賠償之。損害之概念應依照歐盟法院之判例，以能完全反映本指令所欲達成之目標作較寬鬆之解釋。

This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to processing that is unlawful or that infringes the provisions adopted pursuant to this Directive it also covers processing that infringes implementing acts adopted pursuant to this Directive. Data subjects should receive full and effective compensation for the damage that they have suffered.
惟此不應損及就違反歐盟法或會員國法所定其他規則所生損害為任何主張之權利。當涉及違法或違反本指令所採納規定之資料處理，其亦應涵蓋對依照本指令所通過之施行法的違反。資

[10] Council Directive 77/249/EEC of 22 March 1977 to facilitate the effective exercise by lawyers of freedom to provide services (OJ L 78, 26.3.1977, p. 17).
歐盟理事會於 1977 年 3 月 22 日就促進律師有效行使職務以提供服務之自由所制定之歐盟理事會第 77/249/EEC 號指令（官方公報 L 類第 78 期，1977 年 3 月 26 日，第 17 頁）。

料主體就其等所受損害，應受到充分且有實效之賠償。

(89) Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties.

(89) 對任何違反本指令之自然人或法人應予處罰，不論係由私法或公法管制。會員國應確保該處罰係有效、適當且具懲戒性，且應採取一切措施來執行該處罰。

(90) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[11].

(90) 為確保本指令施行之一致狀態，執委會應被賦予就下列事項之執行權力：關於第三國、第三國內之領域或特定部門、或國際組織所應提供之適當保護程度，互助之格式及程序，以及對監管機關間及監管機關與執委會間透過電子方式資訊交換之安排。此等權力應依照歐洲議會及歐盟理事會之歐盟規則第 182/2011 號 [12] 行使之。

[11] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
歐洲議會及歐盟理事會於 2011 年 2 月 16 日關於會員國之委員會行使執行權力之控制機制的規範與一般原則（官方公報 L 類第 55 期，2011 年 2 月 28 日，第 13 頁）。

(91) The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and on the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, given that those acts are of a general scope.

(91) 於通過關於第三國、第三國內之領域或特定部門或國際組織所應提供之適當保護程度、互助之格式及程序，以及對監管機關間及監管機關與委員會間透過電子方式資訊交換之安排之施行法時，應使用檢驗程序。但該等法令以一般法為限。

(92) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, a territory or a specified sector within a third country, or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(92) 當第三國、第三國內之領域或特定部門、或國際組織無法確保充足程度之保護，且有急迫理由者，在合理適當之情況下，執委會應採取立即生效之施行法。

(93) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(93) 因本指令之目的，亦即保護個人之基本權及自由，特別是個人資料受保護之權利，並確保在歐盟境內之主管機關間個人資料之自由交換，尚無法由會員國充分地達成，且行動之規模或效果較能在歐盟層級被達成，故歐盟得依歐盟條約第 5 條所訂定之輔助性原則採取措施。依同條訂定之比例性原則，本指令為達成該等目的，不得超過必要之程度。

(94) Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA [12], or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[13].

(94) 於本指令通過前，經歐盟通過於刑事事務之司法合作及警方合作領域中，規範會員國間個人資料之處理或進入會員國受指定機關依照條約所建立之資訊系統等法令的特訂條款應保持不受

---

[12] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).
2008 年 6 月 23 日歐盟理事會決議第 2008/615/JHA 號關於增加尤其為打擊恐怖主義及跨境犯罪之跨境合作（官方公報 L 類第 210 期，2008 年 8 月 6 日，第 1 頁）。

[13] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1).
2000 年 5 月 29 日之議會法案依照歐盟條約第 34 條，訂定歐盟會員國間刑事事務互助公約（官方公報 L 類第 197 期，2000 年 7 月 12 日，第 1 頁）。

影響，例如關於依照歐盟理事會決議第 2008/615/JHA 號 [12] 所適用之個人資料保護特別規定，或歐盟會員國間刑事事務互助公約第 23 條 [13]。

Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data be ensured in a consistent manner throughout the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of those specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

因憲章第 8 條以及歐洲聯盟運作條約第 16 條要求對基本權之保護在歐盟境內應以一致之方式來確保，執委會應評估有關本指令與其他早於本指令，規定會員國間個人資料之處理或接近使用會員國受指定之機關依照條約所建立之資訊系統而採用之法令，以評估此等特別規範依本指令調整之需求。於適當時，執委會應提案以確保有關個人資料處理一致之法律規範。

(95) In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked.

(95) 為確保在歐盟境內對個人資料全面且一致之保護，會員國間早於本指令生效前所締結，且遵循本指令生效日以前已適用之相關歐盟法的國際協定應繼續有效，直至被修正、取代或廢除為

止。

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force.

(96) 會員國應被允許在本指令生效日以後不超過兩年之時間內作調整。在該日前已開始進行之資料處理應在本指令生效日後兩年內進行調整以與本指令一致。

However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing.

然而，當該等處理係遵循在本指令生效日前已適用之歐盟法時，本指令關於監管機關事前諮詢之要求不應適用於在該日已開始進行之處理活動，但以就其本質而言該等要求在資料處理前已被達成者為限。

Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

當會員國使用在本指令生效日後已滿七年之較長實行期間以達成早於該日建立之自動化處理系統之登記義務，控管者或處理者應設有有效之方法以展示資料處理之合法性，使其能自我監控，並確保資料之完整性及安全性，例如登記或其他形式之紀

錄。

(97) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council[14].

(97) 本指令不影響歐洲議會及歐盟理事會之歐盟指令第 2011/93/EU 號[14]所規定關於打擊兒童性虐待與性剝削及兒童色情業之規範。

(98) Framework Decision 2008/977/JHA should therefore be repealed.

(98) 因此，框架決定第 2008/977/JHA 號應被廢止。

(99) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(99) 依歐盟條約及歐洲聯盟運作條約附錄，即關於英國及愛爾蘭在自由、安全及正義方面之立場之議定書第 21 號第 6a 條，當進行之活動係在歐洲聯盟運作條約第三部分第五篇第四章及第五章之範圍內，即英國及愛爾蘭不受關於刑事事務司法合作或警

---

[14] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
歐洲議會及歐盟理事會於 2011 年 12 月 13 日就打擊兒童性虐待與性剝削及兒童色情業制定歐盟指令第 2011/93/EU 號，並廢止理事會框架決議第 2004/68/JHA 號（官方公報 L 類第 335 期，2011 年 12 月 17 日，第 1 頁）。

方合作之形式規定之拘束而被要求遵循歐洲聯盟運作條約第 16 條之規定時，英國及愛爾蘭不受本指令關於會員國個人資料處理規定之拘束。

(100) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, as annexed to the TEU and to the TFEU, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, is to decide within six months after adoption of this Directive whether it will implement it in its national law.

(100) 依作為歐盟條約及歐洲聯盟運作條約附錄，關於丹麥之立場之議定書第 22 號第 2 條及第 2a 條，當進行之活動係在歐洲聯盟運作條約第三部分第五篇第四章或第五章之範圍內時，丹麥不受本指令關於會員國個人資料處理所設之規範或其適用的拘束。因本指令立基於申根既有規範，在歐洲聯盟運作條約第三部分第五篇下，依據該議定書第 4 條，丹麥得於本指令通過後六個月內決定是其是否在該內國法中實行本指令。

(101) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[15].

(101) 關於冰島及挪威，如同歐盟理事會、冰島共和國及挪威王國所

[15] OJ L 176, 10.7.1999, p. 36.
官方公報 L 類第 176 期，1999 年 7 月 10 日，第 36 頁。

締結關於該二國實行、適用及發展申根既有規範聯盟之協定[15]，本指令構成申根既有規範規定之發展。

(102) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[16]

(102) 關於瑞士，依據歐盟、歐洲共同體與瑞士聯邦間關於瑞士聯邦實行、適用及發展申根既有規範聯盟之協定[16]，本指令構成申根既有規範規定之發展。

(103) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[17].

(103) 關於列支敦士登，依據歐盟、歐洲共同體、瑞士聯邦及列支敦士登侯國關於列支敦士登侯國加盟歐盟、歐洲共同體與瑞士聯邦間關於瑞士聯邦實行、適用及發展申根既有規範聯盟協定之議定書[17]，本指令構成申根既有規範規定之發展。

(104) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in

---

[16] OJ L 53, 27.2.2008, p. 52.
官方公報 L 類第 53 期，2008 年 2 月 27 日，第 52 頁。

[17] OJ L 160, 18.6.2011, p. 21.
官方公報 L 類第 160 期，2011 年 6 月 18 日，第 21 頁。

particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(104) 本指令尊重基本權並遵守歐洲聯盟運作條約明定受憲章承認之原則，特別是尊重私人及家庭生活、個人資料保護、有效救濟及受公正審判之權利。對該等權利之限制係根據憲章第 52 條第 1 項，為達成歐盟承認之公眾利益所必要，或為保護他人之權利或自由而為之。

(105) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition measures. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(105) 依會員國及執委會 2011 年 9 月 28 日就解釋性文件之聯合政治聲明，在正當情況下，會員國同意就其內國法化措施之通知附有一個或數個文件，解釋指令之各部分與該國內國法化措施相應部分之關係。關於本指令，立法者認為該等文件之傳送係為正當。

(106) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012[18].

(106) 歐盟資料保護監督組織依歐盟規則第 45/2001 號第 28 條第 2 項

[18] OJ C 192, 30.6.2012, p. 7.
官方公報 C 類第 192 期，2012 年 6 月 30 日，第 7 頁。

受諮詢；並於 2012 年 3 月 7 日提交其意見[18]。

(107) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access to and rectification or erasure of personal data and restriction of processing in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,

(107) 本指令不應阻礙會員國實踐資料主體行使資訊權、接近使用權、更正或刪除個人資料之權利及對刑事程序中資料處理之限制，以及在國家刑事程序規範中其他可能之限制，

HAVE ADOPTED THIS DIRECTIVE:

已施行本指令：

CHAPTER I General provisions

第一章　總則

Article 1 Subject-matter and objectives

第一條　主旨與立法目的

1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

1. 為規範有關主管機關就預防、調查、偵查及追訴刑事犯罪或執行刑罰目的（包括為維護及預防對於公共安全造成之威脅）所為之個人資料處理，特制定本指令。

2. In accordance with this Directive, Member States shall:

2. 依據本指令，會員國應：

   (a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

   (a) 保護個人基本權與自由，尤其是保護個人資料之權利；及

   (b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

   (b) 確保歐盟境內主管機關間個人資料之流通（如歐盟或會員國法律要求該流通者），不以保護個人資料處理有關理由限制或禁止之。

3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection

of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

3. 關於主管機關處理個人資料對於個人權利及自由之保護，本指令不排除會員國提供較本指令所建立者更高之保護措施。

Article 2 Scope

第二條　範圍

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).

1. 本指令適用於主管機關基於第 1 條第 1 項所定目的所為之個人資料處理。

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. 本指令適用於全部或一部以自動化方式處理之個人資料，且適用於其他非自動化方式處理而構成檔案系統之一部分或旨在構成檔案系統之一部分的個人資料。

3. This Directive does not apply to the processing of personal data:

3. 下列個人資料處理，不適用本指令：

(a) in the course of an activity which falls outside the scope of Union law;

(a) 於歐盟法外治權領域之活動；

(b) by the Union institutions, bodies, offices and agencies.

(b) 歐盟當局、機構、辦事處及局處所為之者。

Article 3 Definitions

第三條　定義

For the purposes of this Directive:

為本指令之目的：

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

(1) 「個人資料」係指有關識別或可得識別自然人（「資料主體」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(2) 「處理」係指對個人資料或個人資料檔案執行任何操作或系列操作，不問是否透過自動化方式，例如收集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀。

(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(3) 「處理限制」係指對於已儲存之個人資料進行標記，以限制其未來之處理。

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict

aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(4) 「建檔」係指對個人資料任何形式之自動化處理，包括使用個人資料來評估與該當事人有關之個人特徵，特別是用來分析或預測有關當事人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動向等特徵；

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(5) 「假名化」係指處理個人資料之方式，使該個人資料在不使用額外資訊時，不再能夠識別出特定之資料主體，且該額外資訊已被分開存放，並以技術及組織措施確保該個人資料無法或無可識別出當事人。

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(6) 「檔案系統」係指依據特定標準可接近使用之個人資料所建構之任何檔案，不問是集中式、分散式或依功能性或地域性分散式之檔案。

(7) 'competent authority' means:

(7) 「主管機關」係指

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(a) 為預防、調查、偵查或追訴刑事犯罪或執行刑罰目的（包

括為維護及預防對於公共安全造成之威脅）之任何主管公務機關；或

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(b) 為預防、調查、偵查或追訴刑事犯罪或執行刑罰目的（包括為維護及預防對於公共安全造成之威脅），會員國法律委託行使公權力之任何其他機構或實體。

(8) 'controller' means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 「控管者」係指單獨或與他人共同決定個人資料處理之目的與方法之主管機關；依照歐盟法或會員國法決定處理之目的及方法，由歐盟法或會員國法律規定控管者或其認定之具體標準；

(9) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 「處理者」係指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構；

(10) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Member State law shall not be regarded as recipients; the

processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 「接收者」係指個人資料被向其揭露之自然人或法人、公務機關、局處或其他機構，不問其是否為第三人。但依據會員國法律，在特定調查框架內可能接收個人資料之公務機關不應視為接收者；該等公務機關所為資料之處理，應依照其處理目的，遵守其所適用之資料保護規則；

(11) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(11) 「個人資料侵害」係指違反安全性導致傳輸、儲存或以其他方式處理之個人資料遭意外或非法破壞、遺失、變更、未獲授權之揭露或接近使用；

(12) 'genetic data' means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(12) 「基因資料」係指涉及當事人遺傳性或突變性之基因特徵之個人資料，尤其是經由當事人生物樣本分析後所取得關於該當事人獨特之生理或健康資訊；

(13) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(13) 「生物特徵識別資訊」係指透過特定技術處理所得關於當事人身體、生理或行為特徵而允許或確認其特定識別性之個人資料，

例如臉部圖像或診斷資料；

(14) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(14) 「涉及健康之資料」係指與當事人之身體或精神健康有關之個人資料，包括提供揭示其健康狀況之醫療照顧服務；

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41;

(15 「監管機關」係指會員國依第 41 條規定成立之獨立公務機關；

(16) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

(16) 「國際組織」係指受國際公法管轄之組織及其附屬機構或依據兩個或多個國家所定協議而成立或以此為基礎所成立之任何其他機構。

CHAPTER II Principles

第二章　原則

Article 4 Principles relating to processing of personal data

第四條　個人資料處理原則

1. Member States shall provide for personal data to be:

1. 會員國應規定個人資料必須：

(a) processed lawfully and fairly;

(a) 合法及公正之處理；

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(b) 蒐集目的須特定、明確及合法，且不得為該等目的以外之處理；

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(c) 適當、相關且不超過其處理目的；

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(d) 正確且必要時應隨時更新；考慮個人資料處理之目的，應採取一切合理措施，確保不正確之個人資料立即被刪除或更正；

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(e) 資料主體之識別資料保存於一定形式，不長於處理目的所必要之期間；

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(f) 處理應以確保個人資料適當安全性之方式為之，包括使用適當之技術上或組織上之措施，以防止未經授權或非法處理，並防止意外遺失、破壞或損壞。

2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

2. 相同或其他控管者基於第 1 條第 1 項所定任一目的處理，而非依該等目的蒐集之個人資料者，須符合：

(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(a) 依照歐盟法或會員國法，該控管者有權為該目的處理個人資料；及

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

(b) 依照歐盟法或會員國法，處理係必要的且與其他目的相當。

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

3. 相同或其他控管者為第 1 條第 1 項所定目的之處理，得包括基於公共利益、科學、統計或歷史用途，但須為資料主體之權利與自由有適當保護措施。

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

4. 控管者應遵守第 1、2 及第 3 項規定，並就其符合負舉證責任。

Article 5 Time-limits for storage and review
第五條　儲存及審查之時間限制

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

會員國應規定刪除個人資料或定期審查儲存個人資料必要性所建立之適當時間限制。程序措施應確保遵守該等時間限制。

Article 6 Distinction between different categories of data subject
第六條　資料主體不同類型之區別

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

會員國應規定控管者（於可適用且有可能時）就不同類型資料主體之個人資料建立清楚之區別，例如：

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(a) 有充分理由相信其已涉犯或將涉犯刑事犯罪之人；

(b) persons convicted of a criminal offence;

(b) 受刑事判決定罪之人；

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(c) 刑事犯罪之受害者或基於特定事實有理由相信其可能成為刑事犯罪受害者之人；及

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

(d) 刑事犯罪之其他關係人，例如於與該刑事犯罪有關之調查或其後之刑事訴訟程序中可能被傳喚作證之人、可提供關於刑事犯罪資訊之人、或第 a 點及第 b 點所定之人的聯絡人或協助者。

Article 7 Distinction between personal data and verification of quality of personal data

第七條　個人資料之區別及個人資料之品質驗證

1. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.

1. 會員國應規定事實性之個人資料盡可能與個人鑑別之個人資料予

以區別。

2. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

2. 會員國應規定主管機關採取一切合理措施以確保不正確、不完整或不合時宜之個人資料不受傳輸或近用。為此，各主管機關於可行之情況下，於傳輸或使個人資料可供使用前，應核實個人資料之品質。所有個人資料之傳輸，應盡可能增加必要之資訊，使接收主管機關得以評估個人資料之正確性、完整性及可靠性以及該等個人資料之更新程度。

3. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

3. 如發現不正確之個人資料已被傳輸或個人資料遭非法傳輸者，應及時通知接收者。於此情況，個人資料應依據第 16 條規定予以更正或刪除或限制處理。

Article 8 Lawfulness of processing
第八條　處理之合法性

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task

carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

1. 會員國應規定，僅有為第 1 條第 1 項所定目的，且主管機關為執行職務所需之必要範圍內，並依據歐盟法或會員國法所為之處理始為合法。

2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

2. 規定本指令範圍內之處理之會員國法律，應至少具體化規定處理之客體、欲處理之個人資料及處理之目的。

Article 9 Specific processing conditions

第九條　特別處理條件

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

1. 主管機關為第 1 條第 1 項所定目的蒐集之個人資料，不得為第 1 條第 1 項規定以外之目的處理，但該處理係經歐盟法或會員國法授權者，不在此限。為其他目的所為之個人資料處理，應適用歐盟規則第 2016/679 號，但非屬於歐盟法律範圍內所為之處理活動者，不在此限。

2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls

outside the scope of Union law.

2. 會員國法律委託主管機關履行第 1 條第 1 項所定目的以外之任務者，歐盟規則第 2016/679 號應適用於該等目的之處理，包括基於公共利益、科學或歷史研究目的或統計目的者，但非屬於歐盟法律範圍內所為之處理活動者，不在此限。

3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.

3. 傳輸主管機關所適用之歐盟法或會員國法就處理定有特別條件者，會員國應規定傳輸主管機關通知個人資料之接收者有關該等條件及遵守該等條件之要求。

4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

4. 會員國應規定傳輸主管機關不得將第 3 項所定特別條件適用於其他會員國境內之接收者或或依照歐洲聯盟運作條約第五篇第四章、第五章設立，而未在該主管機關所屬會員國中適用類似之資料傳輸之局處、辦事處及機構。

Article 10 Processing of special categories of personal data
第十條　特殊類型之個人資料處理

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a

natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:
揭露種族或人種、政治意見、宗教或哲學信仰或貿易聯盟會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關個人資料之處理，僅於嚴格必要之情況下，且須遵守對於資料主體權利及自由之適當保護措施者，始得允許，並限於：

(a) where authorised by Union or Member State law;
(a) 經歐盟法或會員國法授權者；
(b) to protect the vital interests of the data subject or of another natural person; or
(b) 為保護資料主體或他人之重大利益者；或
(c) where such processing relates to data which are manifestly made public by the data subject.
(c) 該處理係涉及由資料主體明顯已自行公開之資料。

Article 11 Automated individual decision-making
第十一條　個人化之自動決策

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.
1. 會員國應規定僅基於自動化處理（包括建檔）所做成而對資料主體產生法律效果或類似之重大影響之決策應予禁止，但經控管者受拘束之歐盟法或會員國法授權，且為該資料主體之權利及自由提供適當安全保護措施者（至少有權對控管者部分為人為參與），

不在此限。

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

2. 本條第 1 項所定決策不得係基於第 10 條所定之特殊類型之個人資料，且應實施適當保護措施以確保資料主體之權利及自由及正當利益。

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

3. 依據歐盟法，應禁止就第 10 條所定之特殊類型之個人資料而造成對個人歧視之建檔。

CHAPTER III Rights of the data subject

第三章　資料主體之權利

Article 12 Communication and modalities for exercising the rights of the data subject

第十二條　資料主體為行使其權利之溝通及管道

1. Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

1. 會員國應規定控管者採取適當措施，以簡明、透明、易懂且方便取得之格式，並採用清楚簡易之語言，提供第 13 條所定之任何資訊及第 11 條、第 14 條至第 18 條及第 31 條所定關於對資料主體所為處理之任何溝通。該資訊應以任何適當方式提供，包括電子格式。原則上，控管者應以與請求相同之形式提供資訊。
2. Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.
2. 會員國應規定控管者促使資料主體依照第 11 條及第 14 條至第 18 條規定行使其權利。
3. Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.
3. 會員國應規定控管者以書面形式通知資料主體關於其請求之後續行動，不得無故遲延。
4. Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
4. 會員國應規定依第 13 條所提供之資訊及依第 11 條、第 14 條至第 18 條及第 31 條所定任何溝通及採取之任何行動，應無償提供之。如資料主體之請求明顯無理由或過度者，尤其是基於該等請求過於重複者，控管者得：
   (a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or
   (a) 考量所要求提供之資訊或溝通或採取行動之行政成本，收取適當費用；或
   (b) refuse to act on the request. The controller shall bear the burden of

demonstrating the manifestly unfounded or excessive character of the request.

(b) 拒絕該請求。控管者應就該請求之明顯無理由或過度性負舉證責任。

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

5. 如控管者對於當事人依照第 14 條或第 16 條提出請求之資料主體身分有合理懷疑者，控管者得要求提供為確認該資料主體身分所必要之額外資訊。

Article 13 Information to be made available or given to the data subject

第十三條　可供使用或提供予資料主體之資訊

1. Member States shall provide for the controller to make available to the data subject at least the following information:

1. 會員國應規定控管者應使資料主體至少得取得以下資訊：

(a) the identity and the contact details of the controller;

(a) 控管者之身分及聯繫方式；

(b) the contact details of the data protection officer, where applicable;

(b) 資料保護員（如適用）之聯繫方式；

(c) the purposes of the processing for which the personal data are intended;

(c) 所欲處理之個人資料之處理目的；

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

(d) 向監管機關提起申訴之權利及該監管機關之聯繫方式；

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of

processing of the personal data concerning the data subject.

(e) 向控管者請求接近使用及更正或刪除及限制處理與資料主體相關個人資料之權利。

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

2. 除第 1 項所定資訊外，會員國應以法律規定控管者於特定情況下，應提供資料主體下列進階資訊以實現其權利：

(a) the legal basis for the processing;

(a) 處理之法律依據；

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(b) 個人資料將被儲存之期間，或如告知期間不可能者，確定該期間所採用之標準；

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(c) 個人資料之接收者類型，包括第三國或國際組織（如適用）；

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

(d) 必要之進階資訊，尤其蒐集係於該資料主體不知情之情況下所為之者。

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

3. 會員國為下列目的，得採取立法措施以延緩、限制或排除適用依

第 2 項規定提供資料主體之資訊，只要該措施在民主社會下符合必要性及比例性，並應注意基本權及相關個人之正當利益：

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(a) 避免阻礙官方或依法之詢問、調查或程序；

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(b) 避免妨害對刑事犯罪之預防、偵查、調查或追訴或刑罰之執行；

(c) protect public security;

(c) 保護公共安全；

(d) protect national security;

(d) 保護國家安全；

(e) protect the rights and freedoms of others.

(e) 保護他人之權利及自由。

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

4. 會員國得採取立法措施，以決定全部或部分屬於第 3 項所列任何一點之處理類型。

Article 14 Right of access by the data subject

第十四條　資料主體之接近使用權

Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

依據第 15 條規定，會員國應規定資料主體有權向控管者確認其個人資料是否正被處理，於此情形者，資料主體應有權接近使用其個人資料

及下列資訊：

(a) the purposes of and legal basis for the processing;

(a) 處理之目的及其法律依據；

(b) the categories of personal data concerned;

(b) 個人資料所涉及之類型；

(c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;

(c) 已揭露或將揭露之個人資料接收者或接收者類型，尤其是在第三國境內或國際組織之接收者；

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(d) 如可能，個人資料將被儲存之預期期間，或如告知期間不可能者，確定該期間所採用之標準；

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

(e) 向控管者請求更正或刪除或限制處理與資料主體相關個人資料之權利；

(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

(f) 向監管機關提起申訴之權利及該監管機關之聯繫方式；

(g) communication of the personal data undergoing processing and of any available information as to their origin.

(g) 處理個人資料之聯繫過程及關於其來源之任何可得資訊。

Article 15 Limitations to the right of access

第十五條 接近使用權之限制

1. Member States may adopt legislative measures restricting, wholly or

partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

1. 會員國為下列目的，得採取立法措施以全部或部分限制資料主體接近使用其等之個人資料，只要該措施在民主社會下符合必要性及比例性，並應注意基本權及相關個人之正當利益：
   (a) avoid obstructing official or legal inquiries, investigations or procedures;
   (a) 避免阻礙官方或依法之詢問、調查或程序；
   (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   (b) 避免妨害對刑事犯罪之預防、偵查、調查或追訴或刑罰之執行；
   (c) protect public security;
   (c) 保護公共安全；
   (d) protect national security;
   (d) 保護國家安全；
   (e) protect the rights and freedoms of others.
   (e) 保護他人之權利及自由。
2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.
2. 會員國得採取立法措施，以決定全部或部分屬於第 1 項所定第 a 點至第 e 點之處理類型。
3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the

reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

3. 關於第 1 項及第 2 項所定情形，會員國應規定控管者就任何對接近使用之拒絕或限制及該拒絕或限制所據理由，以書面通知資料主體，不得無故遲延。如提供該資訊會與第 1 項所定目的相牴觸者，該等資訊得予省略。會員國應規定控管者通知資料主體關於其向監管機關提出申訴或尋求司法救濟之可能性。

4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

4. 會員國應規定控管者紀錄該決定所依據之事實上及法律上之理由。該資訊應提供予監管機關。

Article 16 Right to rectification or erasure of personal data and restriction of processing

第十六條　個人資料之更正權或刪除權及限制處理權

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

1. 會員國應規定資料主體有權使控管者更正其不正確之個人資料，不得無故拖延。考量到處理之目的，會員國應規定資料主體有權完整化其有欠缺之個人資料，包括以提供補充說明之方式。

2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to

obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

2. 如處理違反第 4 條、第 8 條或第 10 條規定，或控管者依其受拘束之法定義務應刪除個人資料者，會員國應要求控管者刪除個人資料，不得無故拖延，並規定資料主體有權使控管者刪除其個人資料，不得無故拖延。

3. Instead of erasure, the controller shall restrict processing where:

3. 除刪除外，有下列任一情形者，控管者應限制處理：

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(a) 資料主體爭執其個人資料之正確性，且其正確性與否無法被驗證者；或

(b) the personal data must be maintained for the purposes of evidence.

(b) 基於證據之目的，該個人資料必須被留存者。

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

依第一款第 a 點規定限制處理者，控管者於取消處理限制前，應通知資料主體。

4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

4. 會員國應規定控管者就任何對限制或刪除個人資料或限制處理之拒絕及該拒絕所據理由，以書面通知資料主體。會員國為下列目的，得採取立法措施以全部或部分限制提供該等資訊之義務，只要該措施在民主社會下符合必要性及比例性，並應注意基本權及相關個人之正當利益：

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(a) 避免阻礙官方或依法之詢問、調查或程序；

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(b) 避免妨害對刑事犯罪之預防、偵查、調查或追訴或刑罰之執行；

(c) protect public security;

(c) 保護公共安全；

(d) protect national security;

(d) 保護國家安全；

(e) protect the rights and freedoms of others. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

(e) 保護他人之權利及自由。會員國應規定控管者通知資料主體關於其向監管機關提出申訴或尋求司法救濟之可能性。

5. Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

5. 會員國應規定控管者將不正確個人資料之更正傳達予產生該資料之主管機關。

6. Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3,

provide for the controller to notify the recipients and that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

6. 個人資料已被更正或刪除或依第 1 項、第 2 項及第 3 項規定限制處理者，會員國應規定控管者通知接收者及規定接收者應更正或刪除個人資料或於其責任範圍內限制該資料之處理。

Article 17 Exercise of rights by the data subject and verification by the supervisory authority

第十七條　資料主體之權利行使及監管機關之驗證

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

1. 於第 13 條第 3 項、第 15 條第 3 項及第 16 條第 4 項所定情形者，會員國應採取措施，規定資料主體之權利亦得由主管監管機關行使之。

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

2. 會員國應規定控管者通知資料主體關於第 1 項所定透過監管機關行使其權利之可能性。

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

3. 依第 1 項規定行使權利之情形，監管機關至少應告知資料主體關於監管機關已為之所有必要之核實或檢驗。

Article 18 Rights of the data subject in criminal investigations and proceedings

第十八條　資料主體於刑事調查及程序中之權利

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

當司法判決或紀錄或案件檔卷中所涉及之個人資料，於刑事調查及法院程序之過程中被處理者，會員國得依會員國法律，就第 13 條、第 14 條及第 16 條所定權利之行使予以規定。

CHAPTER IV Controller and processor

第四章　控管者及處理者

Section 1 General obligations

第一節　一般義務

Article 19 Obligations of the controller

第十九條　控管者之義務

1. Member States shall provide for the controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

1. 會員國應規定控管者，考量處理之性質、範圍、內容及目的以及

當事人之權利及自由所受之諸多可能且嚴重之風險，並實施適當科技化且有組織的措施以確保並得證明其處理符合本指令規定。該等措施應得予審視，且必要時應予更新。

2. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

2. 與處理活動相適當之情況下，第 1 項所定措施應包括控管者適當資料保護政策之實施。

Article 20 Data protection by design and by default

第二十條　藉設計及預設之資料保護

1. Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.

1. 會員國應規定控管者，考量現有技術、執行成本以及處理之性質、範圍、內容及目的以及處理對當事人之權利及自由所生諸多可能且嚴重之風險，不問係在決定處理方式時或係在處理中，實施適當之科技化且有組織的措施，例如假名化，且該等措施旨在實現資料保護原則，如資料最少蒐集原則，並採取有效方式且將必要保護措施納入處理程序，以符合本指令之要求並保護資料主體之權利。

2. Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

2. 會員國應規定控管者實施適當之科技化且有組織的措施，以確保在預設情況下，僅處理特定目的且必要限度範圍內之個人資料。該義務適用於所蒐集之個人資料之數量、處理之程度、儲存之期間及其可接近使用性。尤其是，該等措施於預設情況下，應確保個人資料不能經由人為干預而遭不特定人之接近使用。

Article 21 Joint controllers

第二十一條　共同控管者

1. Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

1. 兩個或兩個以上控管者共同決定處理之目的及方式時，會員國應規定其等為共同控管者。共同控管者應以透明之方式，彼此間安排，確定其各自遵守本指令所定之責任，尤其是關於資料主體行

使其權利及其各自對於第 13 條所定提供資訊所負之責任，但控管者受拘束之歐盟法或會員國法已就控管者各自之責任定有明文者，不在此限。該安排得指定資料主體之聯絡對口。會員國得指定任一共同控管者擔任資料主體行使其權利時之單一聯絡對口。

2. Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

3. 不問第 1 項所定安排之條款為何，會員國得規定資料主體依據本指令對任一控管者行使其權利。

Article 22 Processor

第二十二條　處理者

1. Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

1. 處理係由控管者之代表所為者，會員國應規定控管者僅得任用提供充足保證會實施適當之科技化且有組織的措施、使處理符合本指令所定要求、並確保資料主體權利保障之處理者。

2. Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

2. 會員國應規定，除經控管者事先個案或一般書面授權外，處理者不得複委任其它處理者。在一般書面授權情況下，處理者應通知

控管者關於增加或替換其他處理者之任何預期變化，從而給予控管者對該等變化提出異議之機會。

3. Member States shall provide for the processing by a processor to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

3. 會員國應規定處理者所為處理應受契約或歐盟法或會員國法之其他立法之拘束，該等規定對於處理者及控管者具有拘束力，並規定處理標的及處理期間、處理之本質與目的、個人資料之類型及資料主體之類別以及控管者之義務及權利。該契約或其他立法尤其應規定處理者：

(a) acts only on instructions from the controller;

(a) 僅得依據控管者之指示行事；

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(b) 確保被授權處理個人資料者已承諾保密或具備適當之法定保密義務；

(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(c) 以任何適當措施，協助控管者確保遵守關於資料主體權利之規定；

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(d) 於提供資料處理之服務結束後，依控管者之選擇，向控管者刪除或移轉所有個人資料，並刪除現有副本，但歐盟法或會員國法要求儲存該等個人資料者，不在此限；

(e) makes available to the controller all information necessary to demonstrate compliance with this Article;

(e) 向控管者提供證明遵守本條規定所需之一切資訊；

(f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

(f) 遵守第 2 項及第 3 項所定委任其它處理者之要件。

4. The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

4. 第 3 項所定契約或其他立法應以書面為之，包括電子形式。

5. If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

5. 如處理者決定處理之目的與方式違反本指令者，該處理者應被視為係該處理之控管者。

Article 23 Processing under the authority of the controller or processor

第二十三條　控管者或處理者之處理權限

Member States shall provide for the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

會員國應規定處理者及基於控管者或處理者權限而接近使用個人資料之任何行為人，非基於控管者之指示者，不得處理該等個人資料，但歐盟法或會員國法另有規定者，不在此限。

Article 24 Records of processing activities

第二十四條　處理活動之紀錄

1. Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

1. 會員國應規定控管者應維護其負責之所有類別處理活動之紀錄。該紀錄應包含下列所有資訊：

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(a) 控管者以及共同控管者（如適用）及資料保護員之名稱及聯絡方式；

(b) the purposes of the processing;

(b) 處理目的；

(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(c) 個人資料已對其或將對其揭露之接收者類型，包括第三國或國際組織之接收者；

(d) a description of the categories of data subject and of the categories of personal data;

(d) 資料主體類別及個人資料類型之描述；

(e) where applicable, the use of profiling;

(e) 建檔之用途（如適用）；

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(f) 將個人資料移轉至第三國或國際組織之類型（如適用）；

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

(g) 處理活動之法律依據之描述，包括欲對該個人資料所為之移轉。

(h) where possible, the envisaged time limits for erasure of the different categories of personal data;

(h) 刪除不同類型之個人資料之預設時間上限（如可能）；

(i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

(i) 第 29 條第 1 項所定科技化且有組織之安全措施之概述（如可能）；

2. Member States shall provide for each processor to maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

2. 會員國應規定各處理者維護其代控管者進行各類別處理活動之紀錄，包括：

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

(a) 各控管者及代各控管者進行處理之一個或多個處理者及該各控管者及資料保護員（如適用）之名稱及聯絡方式；

(b) the categories of processing carried out on behalf of each controller;

(b) 代各控管者進行之處理類型；

(c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(c) 依照該控管者之明確指示將個人資料移轉至第三國或國際組織（如適用），包括指明該第三國或國際組織；

(d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

(d) 第 29 條第 1 項所定科技化且有組織之安全措施之概述（如可能）。

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
3. 第 1 項及第 2 項所定紀錄應以書面為之，包括電子形式。

The controller and the processor shall make those records available to the supervisory authority on request.
控管者及處理者應依監管機關之要求提供紀錄。

Article 25 Logging
第二十五條　日誌

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.
1. 會員國應規定日誌至少在下列處理活動中被保存於自動處理系統：蒐集、更正、諮詢、包括移轉之揭露、整合及刪除。諮詢及揭露之日誌應盡可能得以確定該等處理活動之正當性、日期及時間、經諮詢或揭露個人資料之個人身分及接收該個人資料之接收者身分。
2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.
2. 日誌應僅能使用於驗證處理之合法性、自我監控、確保個人資料完整性與資料安全性、以及刑事程序。
3. The controller and the processor shall make the logs available to the supervisory authority on request.
3. 控管者及處理者應依監管機關之要求提供該等日誌。

Article 26 Cooperation with the supervisory authority

第二十六條　與監管機關之合作

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

會員國應規定控管者及處理者依要求與監管機關合作執行其職務。

Article 27 Data protection impact assessment

第二十七條　資料保護影響評估

1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

1. 於特別使用新科技之處理方式，且考量該處理之本質、範圍、使用情形及目的後，認為該處理可能導致自然人之權利及自由的高度風險時，會員國應規定控管者於處理前實行該處理對於個人資料保護之影響評估。

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

2. 第 1 項所定之評估應至少包括擬採用處理活動之概述、對於資料主體之權利及自由之風險評估、應對風險之方式、保護措施、保全措施及確保個人資料保護及符合本指令考慮資料主體及其他相

關人員之權利及合法利益之機制。

Article 28 Prior consultation of the supervisory authority

第二十八條　監管機關之事前諮詢

1. Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:

1. 會員國應規定，於有下列任一情形，且處理將構成其所欲建立之新檔案系統之一部分者，控管者或處理者於處理前諮詢監管機關：

(a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(a) 第 27 條所定之資料保護影響評估顯示，若控管者未採取降低風險之措施，該處理將導致高風險者，或

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

(b) 處理之類型，尤其係使用對資料主體之權利及自由具有高風險之新技術、機制或程序者。

2. Member States shall provide for the supervisory authority to be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing.

2. 會員國應規定，於提出將由國會採納之立法措施建議之準備期間，或依該立法措施之管制措施的準備期間，視何者與處理有關，諮詢監管機關。

3. Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

3. 會員國應規定該監管機關建立須依第 1 項規定進行事先諮詢之處

理活動清單。

4. Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

4. 會員國應規定控管者提供監管機關依第 27 條所定之資料保護影響評估及依其要求提供任何其他資訊，以供監管機關評估該處理之遵守情況，特別是對保護資料主體之個人資料及相關保護措施之風險評估。

5. Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

5. 會員國應規定，當監管機關認為本條第 1 項所稱之處理將違反本指令，尤其是當控管者未能完全指出或減低風險時，監管機關於收受諮詢請求後一定期間（至多 6 周）內，提供書面意見予控管者並視情形予處理者，並得行使其依第 47 條所載之任何權力。該期間可因處理之複雜程度延長 1 個月。監管機關應於收受諮詢請

求後 1 個月內通知控管者並視情形通知處理者上開延期情況及延期原因。

Section 2 Security of personal data
第二節　個人資料之安全性

Article 29 Security of processing
第二十九條　處理之安全性

1. Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

1. 會員國應規定控管者及處理者，考量現有技術、執行成本以及處理之性質、範圍、內容及目的以及處理對當事人之權利及自由所生諸多可能且嚴重之風險，並實施適當之科技化且有組織的措施，以確保對於風險之適當安全程度，尤其是涉及第 10 條特殊類型個人資料之處理。

2. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

2. 關於自動化處理，各會員國應規定控管者或處理者，於評估風險後，實施措施設計為：

   (a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

   (a) 拒絕未經授權之人接近使用處理所用之處理設備（「設備近

用之控管」）；

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(b) 防止未經授權之資料媒介之讀取、複製、修改或移除（「資料媒介之控管」）；

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

(b) 防止未經授權輸入個人資料及擅自檢查、修改或刪除經儲存之個人資料（「儲存控管」）；

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(d) 防止使用資料通訊設備者未經授權使用自動化處理系統（「使用者控管」）；

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

(e) 確保經授權處理自動化處理系統者僅得接近使用其所獲授權之個人資料（「資料接近使用之控管」）；

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

(f) 確保得以驗證及確定可使用資料通訊設備傳輸或可得傳輸予機構（「通訊控管」）；

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

(g) 確保之後得以驗證及確定何等個人資料由何人及於何時輸入至自動處理系統（「輸入控管」）；

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(g) 防止在個人資料移轉期間或在轉換資料媒介期間，未經授權之個人資料之讀取、複製、修改或刪除（「傳輸控管」）；

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(i) 確保安裝之系統在中斷情況下得以回復（「回復」）；

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

(j) 確保系統功能可執行如下，亦即功能故障將會被報告（「可靠性」）且儲存之個人資料不會因為系統之故障而受到破壞（「完整性」）。

Article 30 Notification of a personal data breach to the supervisory authority

第三十條　向監管機關進行個人資料侵害之通報

1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1. 於個人資料侵害發生時，會員國應規定控管者向監管機關通報，不得無故遲延，且如可能，應於發現後 72 小時內通報，但個人資料侵害並無造成對當事人權利及自由之風險者，不在此限。於未於 72 小時內向監管機關通報之情形，通報應附遲延之理由。

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
2. 發現個人資料侵害後，處理者應通報控管者，不得無故遲延。
3. The notification referred to in paragraph 1 shall at least:
3. 第 1 項之通報至少應：
   (a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (a) 描述個人資料侵害之本質，如有可能，應包括相關資料主體之類別及大致數量，及相關個人資料紀錄之類型及大致數量；
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (b) 告知資料保護員之姓名及聯絡細節，或其他得獲得更多資訊之聯絡對口；
   (c) describe the likely consequences of the personal data breach;
   (c) 描述個人資料侵害之可能結果；
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
   (d) 描述控管者已採取或預計採取用以處理個人資料侵害之措施，如適當，應包括降低可能不利影響之措施。
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
4. 於目前無法同時提供資訊者，資訊應分階段提供，不得有進一步之無故遲延。
5. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts

relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

5. 會員國應規定控管者記載本條第 1 項所定之任何個人資料侵害，包括與個人資料侵害相關之事實、其影響及已採取之救濟措施。該等記載應得由監管機關查驗是否與本條相符。

6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

6. 當個人資料侵害涉及已被其他會員國之控管者傳輸之個人資料或已被傳輸至其他會員國境內之控管者時，會員國應規定第 3 項所定之資訊須提供予該會員國之控管者，不得無故遲延。

Article 31 Communication of a personal data breach to the data subject

第三十一條　向資料主體為個人資料侵害之溝通

1. Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

1. 於個人資料侵害可能導致當事人權利及自由之高風險時，會員國應規定控管者與資料主體溝通個人資料侵害，不得無故遲延。

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).

2. 本條第 1 項所稱向資料主體之溝通，應以清楚簡易之語言描述個人資料侵害，並至少包括第 30 條第 3 項第 b、c、及 d 點之資訊

及措施。

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

3. 第 1 項所稱向資料主體之溝通，如有符合下列條件之一者，應無須被要求為之：

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(a) 控管者已執行適當之科技化與有組織之措施，且該等措施已適用於受個人資料侵害影響之個人資料，尤其已使未獲授權接近使用之人無法識別個人資料者，如加密；

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(b) 控管者已採取後續措施，確保第 1 項所稱對資料主體權利及自由之高風險已不會實現；

(c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

(c) 涉及不符比例之努力。於此情形，應有公共溝通或類似措施取代之，使資料主體獲相同有效之通知。

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

4. 於控管者尚未向資料主體溝通個人資料侵害時，監管機關得考量

個人資料侵害可能導致高風險，要求控管者進行溝通或認定第 3 項之任一條件已符合。

5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

5. 本條第 1 項所稱向資料主體之溝通，遇有符合第 13 條第 3 項所定條件且有正當事由者，得予延遲、限制或省略。

Section 3 Data protection officer
第三節　資料保護員

Article 32 Designation of the data protection officer
第三十二條　資料保護員之指定

1. Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

1. 會員國應規定控管者指定資料保護員。會員國於法院及其他獨立司法機關行使其基於該義務所生之司法權能時，得豁免之。

2. The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34.

2. 資料保護員應依專業資格，尤其係其於資料保護法律與實踐之專業知識及完成第 34 條所稱職務之能力，指定之。

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

3. 考量主管機關之組織結構與規模，單一一名資料保護員得為多個

主管機關所指定。

4. Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

4. 會員國應規定控管者公告資料保護員之契約細節，並向監管機關溝通之。

Article 33 Position of the data protection officer

第三十三條　資料保護員之職位

1. Member States shall provide for the controller to ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

1. 會員國應規定控管者確保資料保護員適當且及時涉入所有有關個人資料保護之業務。

2. The controller shall support the data protection officer in performing the tasks referred to in Article 34 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

2. 控管者應透過提供為執行職務及維持對個人資料與處理活動之可及性、以及維持其專業知識所必要之資源，支持資料保護員行使第 34 條所稱職務。

Article 34 Tasks of the data protection officer

第三十四條　資料保護員之職務

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

會員國應規定控管者至少就下列職務委任資料保護員：

(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;

(a) 依本指令及其他歐盟法或會員國法之資料保護規定通知並建議控管者及執行其義務之員工；

(b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(b) 監督本指令、其他歐盟法或會員國法之資料保護規定及與個人資料保護相關之控管者政策，包括責任分配、提高認知及工作人員關於處理活動之訓練、以及相關審計之遵循；

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 27;

(c) 於受資料保護影響評估請求時，提供建議，並依第 27 條監督其執行；

(d) to cooperate with the supervisory authority;

(d) 與監管機關合作；

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 28, and to consult, where appropriate, with regard to any other matter.

(e) 於處理相關之議題，包括第 28 條所稱之事前諮詢時，擔任監管機關之連絡對口，並於適當時提供其他事項之諮詢。

CHAPTER V Transfers of personal data to third countries or international organisations

第五章　個人資料移轉至第三國或國際組織

Article 35 General principles for transfers of personal data

第三十五條　移轉個人資料之一般原則

1. Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

1. 會員國應規定，主管機關移轉任何經處理或於移轉至第三國或國際組織後將欲處理之個人資料，包括進一步移轉至第三國或國際組織者，須遵守依據本指令其他規定通過之國家規定，且符合本章所規定之條件，亦即：

   (a) the transfer is necessary for the purposes set out in Article 1(1);

   (a) 移轉係依第 1 條第 1 項所定目的所必要者；

   (b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);

   (b) 個人資料係基於第 1 條第 1 項所定目的移轉至第三國或國際組織身為公務機關之控管者；

   (c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;

(c) 如個人資料係由其他會員國傳輸或提供時，該會員國依其國內法已就該移轉事先授權者；

(d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and

(d) 執委會已依第 36 條規定通過充足程度保護之決定，或欠缺該等充足程度保護決定但已提供或存在第 37 條所定之適當保護措施，或欠缺第 36 條充足保護決定及第 37 條適當保護措施但適用第 38 條所定之例外特定情形者；及

(e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(e) 當進一步移轉至其他第三國或國際組織時，執行原始移轉之主管機關或同一會員國之其他主管機關，於適當考量所有相關因素，包括刑事犯罪之嚴重性、資料原始移轉之目的及進一步轉入之第三國或國際組織對個人資料保護之程度後，授權該進一步移轉。

2. Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data

is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

2. 會員國應規定，未經另一會員國依照第 1 項第 c 點之規定事先授權者，僅得為防止對會員國或第三國或會員國之重要利益或公共安全造成立即及嚴重威脅而必須移轉個人資料時，且無法及時獲得該事先授權者，始得允許該移轉。應立即通知負責事先授權之機關，不得遲延。

3. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.

3. 為確保本指令保證之當事人保護程度不受減損，本章所有條文應有其適用。

Article 36 Transfers on the basis of an adequacy decision
第三十六條　基於充足程度保護決定之移轉

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

1. 會員國應規定，個人資料移轉至第三國或國際組織，僅於執委會決定該第三國、第三國內之領域或特定部門、或國際組織確有充足程度之保護時，方得為之。該移轉不須獲得任何特別授權。

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

2. 於評估保護程度之充足性時，執委會尤其應考量下列因素：

(a) the rule of law, respect for human rights and fundamental freedoms, 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, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;

(a) 法治、對人權與基本自由之尊重、一般與部門之相關立法，包括有關公共安全、防衛、國家安全及刑法、公務機關對個人資料之接近使用權、及該等立法、資料保護規則、專業規則及安全措施之執行，包括個人資料向其他第三國或國際組織進一步移轉，該其他第三國或國際組織之規則、判例法、及有效且可執行之資料主體權利及個人資料受移轉之資料主體有效之行政與司法救濟；

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(b) 第三國內有一個或更多獨立監管機關之存在及有效運作，或對象為國際組織時，確保及執行資料保護規則之遵守，包括充足之執行權，以協助及建議資料主體行使其權利，並與會員國之監管機關合作；及

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

(c) 第三國或國際組織所加入之國際協定，或其他因具法律拘束力之合約或辦法、及從其參與多邊或區域體系而生之義務，尤其是關於個人資料保護者。

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 58(2).

3. 執委會於評估保護之充足程度後，得透過施行法決定第三國、第三國內之領域或單一或多數之特定部門、或國際組織依本條第 2 項之方式確保充足程度保護。施行法應提供定期檢驗機制，至少四年一次，並應考量第三國或國際組織之所有相關發展。施行法應特定其適用之領域及部門，且於得適用時，確認監管機關或本條第 2 項第 b 點所稱之機關。施行法應採行第 58 條第 2 項之檢驗程序。

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the

functioning of decisions adopted pursuant to paragraph 3.

4. 執委會應持續監控可能影響依第 3 項所採決定之運作之第三國與國際組織的發展。

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 58(3).

5. 於現有資訊顯示，尤其依本條第 3 項之檢驗，第三國、第三國內之領域或單一或多數之特定部門、或國際組織不再確保本條第 2 項意義下之充足程度保護時，執委會應於必要程度內透過執行不具溯及既往效力之行為，廢除、修正或凍結本條第 3 項。該等施行法應依第 58 條第 2 項之檢驗程序行之。於具正當理由之緊急情形，執委會應依第 58 條第 3 項之程序立即採用可適用之施行法。

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

6. 執委會應參與與第三國或國際組織之協商，以救濟依第 5 項作成決定之情形。

7. Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and

38.

7. 會員國應規定，第 5 項之決定不損及依據第 37 條及第 38 條規定向第三國、第三國內之領域及特定部門、及國際組織所為之個人資料移轉。

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

8. 執委會應於歐洲聯盟官方公報及網站上，公布已決定或不再確保具充足程度保護之第三國、第三國內之領域及特定部門、及國際組織之名單。

Article 37 Transfers subject to appropriate safeguards

第三十七條　須遵守適當保護措施之移轉

1. In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

1. 於欠缺第 36 條第 3 項之決定時，會員國應規定，有下列任一情形者，個人資料得予移轉至第三國或國際組織：

   (a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

   (a) 有法律拘束力且得執行之辦法中規定了保護個人資料之適當保障措施；

   (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

   (b) 控管者已評估資料移轉之所有環境且認定關於保護個人資料存在適當保護措施。

2. The controller shall inform the supervisory authority about categories

of transfers under point (b) of paragraph 1.

2. 控管者應將第 1 項第 b 點規定之移轉類別通知監管機關。

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

3. 依第 1 項第 b 點規定之移轉，該移轉應有紀錄，且應依監管機關之要求提供紀錄，包括移轉之日期及時間、關於接收主管機關、移轉之理由及經移轉之個人資料之資訊。

Article 38 Derogations for specific situations

第三十八條　特定情形下之例外

1. In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

1. 於欠缺第 36 條之充足程度保護之決定、或欠缺第 37 條之適當保護措施時，會員國應規定，個人資料之移轉或各類型移轉至第三國或國際組織僅應於符合下列條件且有必要時始得進行：

(a) in order to protect the vital interests of the data subject or another person;

(a) 為保護資料主體或他人之重要利益者；

(b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;

(b) 依移轉該個人資料之會員國法律規定，為確保資料主體之合法利益者；

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(c) 為預防對會員國或第三國之公共安全造成直接及嚴重威脅者；

(d) in individual cases for the purposes set out in Article 1(1); or

(d) 基於第 1 條第 1 項所定目的之個案情形者；或

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

(e) 為建構、行使或防禦關於第 1 條第 1 項所定目的之法律上請求之個案情形。

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

2. 如移轉主管機關決定資料主體之基本權及自由優先於第 1 項第 d 點及第 e 點所定移轉之公共利益者，不得移轉個人資料。

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

3. 依第 1 項規定之移轉，該移轉應有紀錄，且應依監管機關之要求提供紀錄，包括移轉之日期及時間、關於接收主管機關、移轉之理由及經移轉之個人資料之資訊。

Article 39 Transfers of personal data to recipients established in third countries

第三十九條　個人資料移轉至設立於第三國之接收者

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established

in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

1. 不適用第 35 條第 1 項第 b 點規定且不排除本條第 2 項所訂之任何國際契約，歐盟法或會員國法得規定第 3 條第 7 項第 a 點所定主管機關，僅於遵守本指令其他規定且該當於下列所有條件時，得按個別具體情況，將個人資料直接移轉至設立於第三國之接收者：

   (a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);

   (a) 基於第 1 條第 1 項規定之目的，移轉主管機關為執行歐盟法或會員國法法定職務所直接必要之移轉；

   (b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

   (b) 移轉主管機關確定所涉資料主體之基本權及自由並未優先於現時必須進行移轉之公共利益；

   (c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

   (c) 移轉主管機關認為，基於第 1 條第 1 項所定目的，移轉至第三國境內之主管機關為無實效或不適當者，尤其因該移轉無法及時執行；

   (d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

   (d) 第三國境內第 1 條第 1 項所定目的之主管機關應受通知，不得無故遲延，但其為無實效或不適當者，不在此限。

   (e) the transferring competent authority informs the recipient of the

specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

(e) 移轉主管機關將特定目的或僅得由其處理個人資料之目的通知接收者，且該等處理係必要者。

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

2. 第 1 項所定國際協約應係會員國與第三國締結關於刑事事務與警方合作之司法合作雙邊或多邊國際協約。

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

3. 移轉主管機關應依本條規定將移轉通知監管機關。

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

4. 於第 1 項所定之移轉，該移轉應有紀錄。

Article 40 International cooperation for the protection of personal data

第四十條　個人資料保護之國際合作

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

對於第三國及國際組織，執委會及會員國應採取適當之措施：

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(a) 發展國際合作機制以促進有效執行個人資料保護之立法；

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through

notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(b) 提供執行個人資料保護之立法上之國際互助，包括透過關於個人資料保護之適當措施與其他基本權利及自由之通知、申訴轉介、調查協助及資訊交換；

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(c) 使利害關係人參與旨在進一步執行個人資料保護之立法上之國際合作之討論及活動；

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

(d) 提升個人資料保護立法與實務之交換與文件紀錄，包括與第三國之管轄衝突。

CHAPTER VI Independent supervisory authorities

第六章　獨立監管機關

Section 1 Independent status

第一節　獨立地位

Article 41 Supervisory authority

第四十一條　監管機關

1. Each Member State shall provide for one or more independent public

authorities to be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

1. 各會員國應設立至少一個獨立公務機關，職司本指令適用之監控，以保護當事人有關個人資料處理之基本權與自由及促進歐盟內個人資料之自由流動（「監管機關」）。

2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

2. 各監管機關應致力於本指令於歐盟之一致適用。為此，監管機關應依第七章之規定互相及與執委會合作。

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

3. 會員國應規定依歐盟規則第 2016/679 號設立之監管機關為本指令所指之監管機關，且承擔本條第 1 項所設立監管機構之任務之責任。

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

3. 於一會員國內設立一個以上之監管機關時，該會員國應指定其一依照第 51 條規定於委員會中代表各監管機關。

Article 42 Independence

第四十二條　獨立

1. Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.

1. 各會員國應規定，各監管機關依本指令完全獨立行使其職權。

2. Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.

2. 會員國應規定，各監管機關之成員依本指令行使職權，不受直接或間接之外部干擾，並不應依循任何人之指示。

3. Members of Member States' supervisory authorities shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

3. 各監管機關之成員不得為與其職務不相容之行為，並不得於其任期內從事任何不相容之兼職，有無報酬不在所問。

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

4. 各會員國應確保各監管機關具備有效行使職權所需之人力、技術及財務資源、辦公室以及基礎設施，包括於委員會因互助、合作及參與所需執行者。

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

5. 各會員國應確保各監管機關選擇並擁有自身之員工，且員工應受該監管機關成員排他之指示。

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

6. 各會員國應確保各監管機關受財務控制，但不得影響其獨立，且應有單獨、公開之年度預算，並得作為國家或聯邦整體預算之一部分。

Article 43 General conditions for the members of the supervisory authority

第四十三條　監管機關成員之一般條款

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

1. 會員國應使其監管機關之各成員由下列單位本於透明程序所任命：

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

— 國會；

— 政府；

— 國家元首；或

— 依會員國法委託設立之獨立機構。

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform their duties and exercise their powers.

2. 各成員應具行使職權之資格、經驗及技能，特別是關於個人資料

保護之領域。

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

3. 成員之職責應依各該會員國法於其任期結束、解任或強制退休時終止。

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

4. 成員僅於有嚴重不當行為或成員不再符合執行職務之資格時，始得解任之。

Article 44 Rules on the establishment of the supervisory authority

第四十四條　監管機關設立之規則

1. Each Member State shall provide by law for all of the following:

1. 各會員國應以法律規定下列所有事項：

(a) the establishment of each supervisory authority;

(a) 各監管機關之設立；

(b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;

(b) 得受任命為各監管機關成員所需之資格與條件。

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(c) 任命各監管機關成員之規則與程序；

(d) the duration of the term of the member or members of each supervisory authority of not less than four years, except for the first appointment after 6 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(d) 各監管機關成員之任期不得少於四年。但為保障監管機關獨立性之必要而採取交錯任期之方式，使 2016 年 5 月 6 日後第一次任命之任期較短者，不在此限；

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(e) 各監管機關成員是否得受再任命，及若是，其任期數；

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

(f) 各監管機關成員及工作人員之義務條款、禁止其任期內與任期後與其職務不相容之行為、兼職及利益、以及停職之規範。

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or the exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Directive.

2. 依歐盟或會員國法，各監管機關之成員及工作人員應於任期內及任期後，對因行使職權知悉之任何機密資料負專業保密義務。於任期內，其專業保密義務尤其應適用於本指令之當事人侵害報告。

Section 2 Competence, tasks and powers
第二節　權限、職務及權力

Article 45 Competence
第四十五條　權限

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

1. 各會員國應規定，各監管機關有權於自己之會員國領域內依本指令執行受指定之職務並行使權力。

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

2. 各會員國應規定，各監管機關無權監督法院就其司法權所為之處理執行。會員國得規定，其監管機關無權監督其他獨立之司法機關就其司法權所為之處理執行。

Article 46 Tasks
第四十六條　職務

1. Each Member State shall provide, on its territory, for each supervisory authority to:

1. 各會員國應規定，各監管機關於其領域內：

   (a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

   (a) 監控及執行依據本指令及其施行措施所通過之規定之適用；

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(b) 提升公眾對有關處理之風險、規則、保護措施及權利之意識及理解；

(c) advise, in accordance with Member State law, the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(c) 依會員國法建議國會、政府及其他機關或機構，關於涉及處理之當事人權利及自由保護之立法及行政措施；

(d) promote the awareness of controllers and processors of their obligations under this Directive;

(d) 提升控管者及處理者對其於本指令之義務之意識；

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(e) 基於請求，提供關於本指令下權利行使之資料予任何資料主體，若適合，與其他會員國之監管機關合作提供；

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(f) 處理資料主體或機構、組織或協會依第 55 條之申訴，並適當程度調查該申訴事項，於合理時間內通知申訴人調查之進度與結果，尤其於進一步之調查或與其他監管機關之協調為必要時；

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

(g) 確認第 17 條規定處理之合法性，並於合理期間內依第 17 該條第 3 項規定將該確認結果或未為確認之理由通知資料主體；

(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;

(h) 與其他監管機關合作，包括分享資訊及互助，以確保本指令適用與執行之一致性；

(i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;

(i) 執行本指令適用之調查，包括其他監管機關或其他公務機關所提供資訊之基礎；

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(j) 於相關發展影響個人資料之保護時監控之，尤其是資訊與通訊科技之發展；

(k) provide advice on the processing operations referred to in Article 28; and

(k) 就第 28 條規定之處理活動提供建議；及

(l) contribute to the activities of the Board.

(l) 協助委員會之活動。

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f)of paragraph 1 by measures such as providing a complaint submission form which can also be completed electronically,

without excluding other means of communication.

2. 各監管機關應透過諸如亦得單以電子方式完成而不須其他溝通方式之申訴提交表格等方式，促進第 1 項第 f 點之申訴提交。

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

3. 各監管機關之職務行使不應向資料主體收取費用，亦不應向資料保護員收取之。

4. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

4. 於請求顯無理由或過度時，尤其於重複情形，監管機關得基於行政成本收取合理費用，或得拒絕處理請求。監管機關應負請求顯無理由或請求過度之舉證責任。

Article 47 Powers

第四十七條　權力

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

1. 各會員國應以法律規定各監管機關具有效之調查權力。該等權力應至少包括自控管者及處理者獲得接近使用其正在處理之一切個人資料及其執行任務所需之一切資訊。

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

2. 各會員國應以法律規定各監管機關具有效之糾正權力，諸如：

(a) to issue warnings to a controller or processor that intended

processing operations are likely to infringe the provisions adopted pursuant to this Directive;

(a) 當欲進行之資料處理可能會違反依本指令所通過之規定時，向控管者或處理者發布警告；

(b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;

(b) 命令控管者或處理者以適當之特定方法及於特定期間內使資料處理符合依本指令所通過之規定，尤其是命令依第 16 條對個人資料之更正或刪除，或對資料處理之限制；

(c) to impose a temporary or definitive limitation, including a ban, on processing.

(c) 課予暫時或終局之限制，包括對資料處理之禁令；

3. Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

3. 各會員國應以法律規定各監管機關具有效之建議權力，依第 28 條之事前諮詢程序建議控管者，及對其國會及政府或依其國內法對其他公共團體、機構及大眾主動或依請求發布針對任何與個人資料保護相關之議題的意見。

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, as set out in Union

and Member State law in accordance with the Charter.

4. 監管機關行使本條賦予之權力應有適當保護措施，包括歐盟法及會員國法依憲章所規定之有效之司法救濟及正當程序。

5. Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

5. 各會員國應有法律規定監管機關應有權力將違反本指令通過之規定者檢送司法機關，並於適當時開啟或參與司法程序，以執行依本指令所通過之規定。

Article 48 Reporting of infringements

第四十八條　違規之報告

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

會員國應規定主管機關建立有效之機制，促進對違反本指令之機密報告。

Article 49 Activity reports

第四十九條　活動報告

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of penalties imposed. Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, the Commission and the Board.

各監管機關應編製年度活動報告，得包括受告知之侵害類型以及採取

之措施類型清單。該等報告應依會員國法之指定提交國會、政府及其他有權機關。該等報告應對大眾、執委會及委員會公開。

CHAPTER VII Cooperation

第七章　合作

Article 50 Mutual assistance

第五十條　互助

1. Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

1. 各會員國應規定其監管機關提供彼此相關資訊並互助以一致地實施並適用本指令，並應訂定相互有效合作之措施。互助應特別包括資訊要求及監督措施，例如要求進行諮詢、檢查及調查。

2. Each Member States shall provide for each supervisory authority to take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

2. 各會員國應規定各監管機關採取所有適當措施，不得無故遲延且不遲於收到請求後一個月內，回覆另一監管機關之請求。該等措施特別得包括傳送關於調查行為之相關資訊。

3. Requests for assistance shall contain all the necessary information,

including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

3. 請求協助應包含所有必要資訊，包括該請求之目的及理由。交換之資訊應僅得用於所請求之目的。

4. The requested supervisory authority shall not refuse to comply with the request unless:

4. 受請求之監管機關不得拒絕接受該請求，除非：

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(a) 其無權處理請求之標的或請求執行之措施；或

(b) compliance with the request would infringe this Directive or Union or Member State law to which the supervisory authority receiving the request is subject.

(b) 接受該請求將違反受請求之監管機關所應遵守之本指令、歐盟法或會員國法。

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

5. 受請求之監管機關應將結果或依其情形將採取之措施的進展狀況通知請求之監管機關，以回應該請求。受請求之監管機關應提供任何拒絕依第 4 項接受請求之理由。

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

6. 受請求之監管機關在一般情形應使用標準化格式，以電子方式提供其他監管機關請求之資訊。

7. Requested supervisory authorities shall not charge a fee for any

action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

7. 受請求之監管機關就其依互助之請求採取之任何行動不得收取費用。監管機關得同意就特別情況下提供互助產生之具體支出之互相補償規範。

8. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

9. 執委會得透過施行細則具體規範本條所述之互助的格式及程序，以及監管機關相互間及監管機關與委員會間以電子方式資訊交換之安排。該施行細則應通過第 58 條第 2 項所述之審查程序。

Article 51 Tasks of the Board

第五十一條　委員會之任務

1. The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in relation to processing within the scope of this Directive:

1. 依據歐盟規則 2016/679 號設立之委員會應在本指令範圍內執行下列與處理有關之一切任務：

   (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

   (a) 就與歐盟境內個人資料保護之任何議題，包括就本指令之任何建議修訂，向執委會提供意見；

   (b) examine, on its own initiative, on request of one of its

members or on request of the Commission, any question covering the application of this Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;

(b) 主動或依其一名成員或執委會之請求，審查涵蓋本指令適用之任何問題並發布指導原則、建議及最佳作法以鼓勵本指令之一致適用。

(c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);

(c) 就第 47 條第 1 項及第 3 項所述措施之適用，為監管機關制定指導原則；

(d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(d) 為確定個人資料侵害並決定第 30 條第 1 項及第 2 項所述之無故遲延，以及控管者或處理者被要求通知該個人資料侵害之特定情況，依本款第 b 點發布指導原則、建議及最佳做法；

(e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);

(e) 在第 31 條第 1 項所述就個人資料侵害可能導致對當事人權利及自由之高風險之情形，依本款第 b 點發布指導原則、建議及最佳做法。

(f) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and

(c);

(f) 審查第 b 點及第 c 點所述指導原則、建議及最佳做法之實際適用；

(g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;

(g) 提供執委會關於第三國、第三國內之領域或一個或多個特定部門或國際組織保護程度適當性之評估，包括評估該第三國、第三國內之領域或特定部門、或國際組織是否不再確保適當程度之保護。

(h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(h) 促進監管機關間之合作、有效之雙邊及多邊資訊交換及最佳作法；

(i) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(i) 促進一般培訓方案並促進監管機關間及在適當時與第三國之監管機關或國際組織之人員交換；

(j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

(j) 促進與全世界之資料保護監管機關間資料保護法律及實踐知識及文件之交換。

With regard to point (g) of the first subparagraph, the Commission

shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

關於第一款第 g 點，執委會應提供委員會一切所需文件，包括與第三國政府關於第三國內之領域或部門，或與國際組織之通信。

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

2. 若執委會要求委員會提供建議，考量該事項之急迫性，得指定一定之時限。

3. The Board shall forward its opinions, guidelines, recommendations and best practices to the Commission and to the committee referred to in Article 58(1) and make them public.

3. 委員會應將其意見、指導原則、建議及最佳作法轉呈執委會及第 58 條第 1 項所述之委員會，並將其公開。

4. The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

4. 執委會應將其依據委員會發布之意見、指導原則、建議及最佳作法所採取之行動通知委員會。

CHAPTER VIII Remedies, liability and penalties

第八章　救濟、義務及處罰

Article 52 Right to lodge a complaint with a supervisory authority

第五十二條　向監管機關提出申訴之權利

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

1. 在不影響任何其他行政或司法救濟之情況下，會員國應規定，如資料主體認為與其有關之個人資料處理違反依本指令通過之規定者，資料主體有權向監管機關提出申訴。

2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.

2. 會員國應規定，如申訴非屬該監管機關依第 45 條第 1 項管轄者，受理申訴之監管機關移送該申訴予主管監管機關，不得無故遲延。

3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

3. 會員國應規定，受理申訴之監管機關依資料主體之請求提供進一步之協助。

4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

4. 資料主體應獲受理申訴之監管機關通知該申訴之過程及結果，包括依第 53 條規定提起司法救濟之可能性。

Article 53 Right to an effective judicial remedy against a supervisory authority

第五十三條　對監管機關提起有效司法救濟之權利

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

1. 在不影響任何其他行政或非司法救濟之情況下，會員國應規定自然人或法人有權對監管機關就其所為具有法律拘束力之處分提起有效司法救濟。

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.

2. 在不影響任何其他行政或非司法救濟之情況下，如第 45 條第 1 項所定之監管主管機關不處理申訴或未於三個月內依照第 52 條規定通知申訴人申訴進展或結果者，資料主體應有權提起有效之司法救濟。

3. Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

3. 會員國應規定對監管機關之訴訟提交於監管機關設立地之會員國法院。

Article 54 Right to an effective judicial remedy against a controller or processor

第五十四條　對於控管者或處理者提出有效司法救濟之權利

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data

subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.
在不影響任何現有之行政或非司法救濟（包括依第 52 條向監管機關提出申訴之權利）之情況下，會員國應規定，如資料主體認為其依本指令所通過之規定所定之權利因未遵守該等規定處理其個人資料而遭受侵害者，資料主體有權提出有效之司法救濟。

Article 55 Representation of data subjects
第五十五條　資料主體之代表

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.
會員國應依照會員國程序法，使資料主體有權委任依照會員國法合法設立、以公益為目的，且在個人資料保護領域活躍之非營利機構、組織或社團，代其就其等之個人資料保護提出申訴、代其行使第 52、53 及 54 條所定之權利。

Article 56 Right to compensation
第五十六條　賠償請求權

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the

controller or any other authority competent under Member State law.
會員國應規定，因非法處理活動或任何違反各國依本指令所通過之規定之行為，造成物質上或非物質上之損害時，任何人應有權依會員國法就其損害自控管者或任何主管機關獲得賠償。

Article 57 Penalties
第五十七條　罰則

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.
會員國應制定違反依本指令所通過之規定所適用之罰則規定，並應採取一切必要措施確保該等規定得予執行。該罰則應有效、適當且具懲戒性。

CHAPTER IX Implementing acts
第九章　施行法

Article 58 Committee procedure
第五十八條　執委會之程序

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
1. 執委會應由依歐盟規則第 2016/679 號第 93 條設立之委員會協助。該委員會應為歐盟規則第 182/2011 號意義範圍內之委員會。
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
2. 於本項情形，歐盟規則第 182/2011 號第 5 條規定應予適用。

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.
3. 於本項情形，歐盟規則第 182/2011 號第 8 條與第 5 條規定應一併適用之。

CHAPTER X Final provisions

第十章　最終條款

Article 59 Repeal of Framework Decision 2008/977/JHA

第五十九條　第 2008/977/KHA 號框架決定之廢止

1. Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.
1. 第 2008/977/JHA 號框架決定自 2018 年 5 月 6 日起廢止。
2. References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.
2. 凡提及第 1 項所稱廢止指令者，應被解釋為係指本指令。

Article 60 Union legal acts already in force

第六十條　已生效之歐盟法規

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

歐盟法規在刑事事務之司法合作及警方合作領域就個人資料保護於 2016 年 5 月 6 日以前生效，規定會員國間之資料處理及接近使用會員國受指定之機關在本指令之範圍內依照條約所建立之資訊系統之特定

規範，應保持不受影響。

Article 61 Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

第六十一條　與在刑事事務之司法合作及警方合作領域已締結之國際協議之關係

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

會員國於 2016 年 5 月 6 日以前締結涉及個人資料移轉至第三國或國際組織，並遵守適用於該日期以前適用之會員國法之國際協議者，其應繼續有效，直到修正、被取代或被廢止。

Article 62 Commission reports

第六十二條　執委會報告

1. By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Directive to the European Parliament and to the Council. The reports shall be made public.

1. 2022 年 5 月 6 日以前，以及往後每四年，執委會應向歐洲議會及歐盟理事會提交關於評價及審查本指令之報告。該等報告應公開。

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.

2. 在第 1 項所述評價及審查之範圍內，執委會應特別檢驗第五章關於將個人資料移轉至第三國或國際組織之適用與運作情形，特別

係依據第 36 條第 3 項及第 39 條通過之裁決。

3. For the purposes of paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities.

3. 為第 1 項及第 2 項之目的，執委會得向會員國及監管機關請求資訊。

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.

4. 在進行第 1 項及第 2 項所述之評價及審查時，執委會應考量歐洲議會、歐盟理事會及其他相關機構或來源之立場及調查結果。

5. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

5. 如有必要，執委會應提交修訂本指令之適當提案，特別是考量資訊科技之發展，以及資訊社會之進展狀況。

6. By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

6. 2019 年 5 月 6 日以前，執委會應審查其他經歐盟通過，規定主管機關依第 1 條第 1 項之目的所為資料處理的法規，包括第 60 條所提及者，以評估該等法規依本指令調整之必要性，並適時提出必要之提案修訂該等法規以確保在本指令範圍內一致之個人資料保護方法。

Article 63 Transposition

第六十三條　轉化

1. Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

1. 會員國應於 2018 年 5 月 6 日以前通過並公告遵守本指令所必要之法律、規則或行政規範。其等應立即通知執委會該等規範之內容。其等應自 2018 年 5 月 6 日起適用該等規範。

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

當會員國通過該等規範，該等規範應提及本指令，或應在該等規範正式公布之場合提及。會員國應決定該等提及應如何為之。

2. By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

2. 在不適用第 1 項之情形，若需花費過鉅之勞力，就 2016 年 5 月 6 日以前建立之自動化處理系統，會員國得特別規定須在 2023 年 5 月 6 日以前符合第 25 條第 1 項之規定。

3. By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the

Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

3. 在不適用本條第 1 項及第 2 項之情形，在例外情況下，若將造成該特定自動化處理系統運作之嚴重困難時，會員國得規定本條第 2 項所稱之自動化處理系統須在該項所指之期限後之特定期限內符合第 25 條第 1 項之規定。相關會員國應告知執委會該等嚴重困難之理由，以及應在該特定期限內符合第 25 條第 1 項規定之理由。該特定期限在任何情況下不得遲於 2026 年 5 月 6 日。

4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

4. 會員國應向執委會通知就本指令所涵蓋範圍該國通過之法律的主要規範內容。

Article 64 Entry into force

第六十四條　生效

This Directive shall enter into force on the day following that of its publication in the Official Journal of the European Union.

本指令應在公布於歐洲聯盟官方公報之日起生效。

Article 65 Addressees

第六十五條　發布

This Directive is addressed to the Member States.

本指令對會員國發布。

Done at Brussels, 27 April 2016.

完成於布魯塞爾，2016 年 4 月 27 日。

For the European Parliament
歐洲議會
The President
主席
M. SCHULZ

For the Council
歐盟理事會
The President
主席
J.A. HENNIS-PLASSCHAERT

國立中央圖書館出版品預行編目資料

歐盟個人資料保護規則 / 財團法人金融聯合徵信中心編輯委員會編 . -- 初版 . -- 臺北市 : 金融聯合徵信 , 民 106.07
面 ; 公分 . --(金融與徵信叢書 ; 77)
中英對照

ISBN 978-986-6478-57-4(平裝)

1. 歐洲聯盟 2. 資訊法規 3. 資訊安全

584.111 106011372

金融與徵信叢書 No. 77

歐盟個人資料保護規則

中華民國一〇六年七月初版

發行者：張 國 銘
編印者：財團法人金融聯合徵信中心編輯委員會
出版者：財團法人金融聯合徵信中心
地 址：台北市重慶南路一段 2 號 10 樓
電 話：(02)2191-0000

JCIC
The Credit Bureau of Taiwan

www.jcic.org.tw

財團法人金融聯合徵信中心
Joint Credit Information Center
100台北市中正區重慶南路一段2號10樓
16F, No. 2, Sec. 1, Chong Ching S. Rd.
Taipei 100, Taiwan, R.O.C
Tel 886-2-21910000

ISBN 978-986-64-7857-4
9 789866 478574