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,

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,

---

* 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。

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

---

[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。

(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 ([1]) 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([1])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) 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

[1] 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）。

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([1]).

(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([1])。

(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

[1] 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）。

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 ([1]) 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([1])所訂定 45/2001 號規則適用於歐盟當局、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

[1] 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）。

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([1]). 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([1])。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, 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

---

[1] 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）。

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([1]), 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.

(21) 本規則不影響歐洲議會及歐盟理事會([1])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。

---

[1] 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）。

(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 ([1]) 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.

(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([1])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

---

[1] 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）。

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 ([1]) 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([1])，控管者事先擬定之同意聲明書，

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

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

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 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

---

號（官方公報 L 類第 95 期，1993 年 4 月 21 日，第 29 頁）。

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 ([1]), 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 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([1])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

---

[1] 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）。

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 ([1]) 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 ([1])，向委員會報告任何相關認定。

(107) The Commission may 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 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.

---

[1] 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）。

(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 ([1]) should not prejudice 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([1])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,

---

[1] 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 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）。

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 ([1]) 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. 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([1])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

---

[1] 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）。

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 ([1]) should apply.

(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([1])應適用之。

---

[1] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, 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）。

(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 ([2]) 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([1])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 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

---

[1] 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)。

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 ([1]).

(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([1])。

(173) This Regulation should apply to all matters concerning the

[1] 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。

protection of fundamental rights and freedoms *vis-à- vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ([2]), 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([1])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：

[1] 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）。