國家發展委員會
NATIONAL DEVELOPMENT COUNCIL

歐盟《個人資料保護規則》簡介

中華民國 107 年 5 月

本簡介主要目的在於介紹歐盟《個人資料保護規則》(General Data Protection Regulation, 以下簡稱 GDPR) 以提供企業、組織及國人參考。

本簡介並非對 GDPR 作出法律解釋或提出法律意見，亦不作為適用 GDPR 的指引。蒐集個資機關應尋求專業意見以評估如何遵循 GDPR。

目錄

GDPR 簡介

歐盟《個人資料保護規則(General Data Protection Regulation, GDPR)》於 2018 年 5 月 25 日生效，依 GDPR 的域外管轄規定，無論是否在歐盟境內設有據點的台灣企業、組織都有可能受到該法律的規範拘束(見下述)，且 GDPR 的行政處罰額度上限極高(最高達 2000 萬歐元或年度全球營收的 4%)，因此，本簡介旨在整理 GDPR 的重要規範，以供台灣企業、組織及國人作為初步參考。

誰適用 GDPR

無論是控管者（controller，決定處理個資之目的及方法之人[1]）或處理者（processor，依控管者指示而處理個資之人[2]），只要經營業務活動需「處理[3]」個人資料，且符合下列三種情形之一，就須適用 GDPR：

- 在歐盟境內設立據點（establishment），且無論處理個資之行為是否發生在歐盟境內[4]。
- 在歐盟境內未設立據點，但對歐盟境內自然人提供商品或服務，無論是否收費[5]。判斷方式例如「網站提供歐盟會員國的官方語言」、「得使用歐元結帳」、「網站中提及歐盟消費者或使用者」等[6]。

---

[1] GDPR, Article4(7), "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"

[2] GDPR, Article4(8), "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

[3] GDPR 規範的「處理(processing)」，與我國個資法之「處理」，定義上有很大的差異，GDPR 第 4 條第 2 項將處理定義為「不論是否透過自動化方式，對個人資料或個人資料檔案執行任何操作或系列操作，例如蒐集、記錄、組織、結構化、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、傳播或以其他方式使之得以調整或組合、限制、刪除或銷毀」，故 GDPR 之處理已包含我國個資法之蒐集、處理與利用等三種行為。

[4] GDPR, Article3(1), "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

[5] GDPR, Article3(2), "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union…"

[6] GDPR, Recital23, "…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

- 在歐盟境內未設立據點，但監控歐盟境內自然人於歐盟內之行為[7]。例如追蹤歐盟境內自然人的網路行為以對該自然人「做出某種決定」、「分析或預測該自然人的喜好、行為或意見」等[8]。

需注意的是，GDPR 在此所稱之自然人並非以「國籍」區分而是以「是否在歐盟境內」作為適用的判斷標準。

---

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."

[7] GDPR, Article3(2), "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: …b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

[8] GDPR, Recital24, "…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."

GDPR 適用重點

1、指派歐盟境內代理人

如果控管者或處理者在歐盟境內沒有設立據點，但須適用 GDPR 時，應以書面委任歐盟境內的代理人（自然人或法人）作為代表[9]，代替或與控管者/處理者一同受理監督機關（Supervisory Authorities）或個資當事人（Data Subjects）關於處理個資行為提出的要求[10]。而此代理人須在「接受商品或服務」或「受監控行為」的歐盟自然人所在國之一設立據點[11]。

不過上述「委任代理人」的義務也有例外，除了公務機關/構不適用外，如考量控管者或處理者處理個資行為的性質、內容、範圍及目的後，可認為僅是偶發性的處理個資，且不涉及大規模處理 GDPR 第 9 條第 1 項規定的特種個資或第 10 條規定的刑事個資，又不太可能對個資當事人的權利或自由產生風險者，即不受上述規定拘束，不須在歐盟委任代理人[12]。

---

[9] GDPR, Article27(1), "Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union."

[10] GDPR, Article27(4), "The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation."

[11] GDPR, Article27(3), "The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are."

[12] GDPR, Article27(2), "The obligation laid down in paragraph 1 of this Article shall not apply to: a) processing which is occasional, does not include, on a large scale,

2、個人資料的定義

2.1 一般個人資料

GDPR 定義的一般個人資料是指「任何與已識別或可識別的自然人（個資當事人）相關之資訊」; 所謂「可識別的自然人」則指「可透過如姓名、身分號碼、地理位置、線上識別符（online identifier）等識別符或該自然人之一或多個特定身體、生理、基因、心理、經濟、文化、社會地位等要素而直接或間接識別之自然人」[13]；在 GDPR 立法理由（Recital）更說明「自然人可能與其裝置、應用程式、工具或通訊協定等提供之線上識別符（例如 IP 位址、cookies 碼、無線射頻識別標籤）關聯（而被識別），此將使該自然人留下得以對其建立檔案並識別身分的軌跡（trace），尤其是與伺服器接收的專屬識別符或其他資訊結合時」[14]。

---

processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or b) a public authority or body."

[13] GDPR, Article4.1, " 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

[14] GDPR, Recital30, "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses,

2.2 特種個人資料

GDPR 定義的特種個人資料是指「揭露人種、血統、政治意見、宗教或哲學信仰、工會身分之資料，以及基因資料、專用以識別自然人的生物特徵資料、健康相關資料或與自然人之性生活與性取向相關之資料」，且原則上禁止處理[15]。

2.3 刑事個人資料

GDPR 定義的刑事個人資料是指「前科與犯罪紀錄」，並規定僅得在公務機關控管，或依歐盟法律或會員國法律對個資當事人的權利及自由設有適當安全維護之規範而允許的前提下，始可處理刑事個資[16]。

---

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."

[15] GDPR, Article9(1), "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[16] GDPR, Article10, "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

3、處理個資的原則[17]

依 GDPR 規定，處理個人資料的行為必須遵循下列原則：

3.1 合法性原則、公平性原則、透明性原則

個人資料應依合法、公平且對個資當事人透明之方式處理。

3.2 目的限制原則

個人資料應依特定、明確且合法之目的而蒐集，並不得以跟蒐集目的不相符的方式處理；但依 GDPR 規定為公共利益、科學或歷史研究、統計等目的之處理不構成與蒐集目的不相符之行為。

[17] GDPR, Article5, "Personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

3.3 個資最小化原則

個人資料之處理應限於與處理目的具有適當性、關聯性及必要性。

3.4 正確性原則

個人資料應保持正確，如有必要應即時更新；依處理之目的，應採取所有合理措施以確保不正確之個資得即時刪除或更正。

3.5 儲存限制原則

個人資料如以得識別個資當事人的形式保存，不應超過處理目的之必要期間；個人資料僅得單純為依 GDPR 規定之公共利益、科學或歷史研究、統計等目的，而於處理目的之必要期間過後，在導入適當的技術上及組織上措施以保障個資當事人之權利及自由的前提下繼續保存。

3.6 完整性原則、機密性原則

個人資料應以能確保適當安全的方式處理，包含以適當的技術上及組織上措施避免未獲授權或違法之處理，以及個資遺失、滅失或毀損。

4、處理個資的法律依據[18]

依 GDPR 規定，必須具備下列法律依據之一，才能合法處理個人資料：

4.1 當事人同意

個資當事人同意控管者基於一個或多個特定目的處理其個人資料。同意之內涵見下 5。

4.2 與當事人有契約（前）關係

處理個資是為了向契約當事人（個資當事人）履行契約所必須者，或在締約前，應個資當事人之要求，所必須採取之步驟。

4.3 為遵守法律義務

處理個資是控管者為遵守法律義務所必須者。

[18] GDPR, Article 6 (1), "Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

4.4 基於重大利益

處理個資是為保護個資當事人或其他自然人之重大利益所必須者。

4.5 基於公共利益

處理個資是為追求公共利益而執行任務或委託控管者行使公權力所必須者。

更多正當利益資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC》。連結見《參考資源》

4.6 基於正當利益

處理個資是控管者或第三人為追求正當利益之目的所必須者，但該個資當事人之利益或基本權與自由所需之個資保護優於前述正當利益時，特別是該個資當事人為兒少時，即不可適用。

更多當事人同意資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on consent under Regulation 2016/679》。連結見《參考資源》

5、當事人同意

5.1 同意的品質

依 GDPR 規定，個資當事人的有效同意是指「個資當事人對於處理與其相關之個人資料，透過聲明（statement）或清楚肯定（clear affirmative）之行為，自願、具體、知情（informed）、明確（unambiguous）作出的任何明示同意之意思表示」[19]。

又 GDPR 立法理由對於「清楚肯定之行為」表示包含「文字聲明（也可以電子文件形式）或口頭聲明」，亦包含「造訪網站時勾選同意」、「對資訊服務（例如影音串流、互動數位電視）選擇不同的技術設定」，相反的，「單純沉默」、「網站預設勾選同意」或其他「不作為」均不構成 GDPR 定義的有效同意[20]。

[19] GDPR, Article4.11, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

[20] GDPR, Recital32, "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

而在評估個資當事人同意的自願性時，應特別考量控管者以「個資當事人同意」作為處理個資的法律依據，但履行雙方契約（或服務條款）並不必然需要處理個人資料時[21]，是否有對個資當事人顯失公平的情況。

5.2 以同意作為處理個資的法律依據

如控管者以個資當事人同意作為處理其個資的法律依據時，控管者應對個資當事人同意之事實負舉證責任[22]。

如個資當事人之同意是併同其他事項所為之書面聲明時，應以明確與其他事項區分的形式向個資當事人請求同意，並使用易懂且便於取得之格式，以及清楚簡白之語言；另該聲明中任何違反 GDPR 之部份均屬無效[23]。

---

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."

[21] GDPR, Article7(4), "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[22] GDPR, Article7(1), "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

[23] GDPR, Article7(2), "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such

5.3 撤回同意

個資當事人有權隨時撤回同意，但其撤回不影響撤回前基於該同意處理個資的合法性；而個資當事人應於同意前即受告知有前述撤回之權；又同意之撤回應與給予同意一樣容易[24]。

a declaration which constitutes an infringement of this Regulation shall not be binding."

[24] GDPR, Article7(3), "The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

6、兒童與少年的同意限制

GDPR 特別注重保護兒童及少年的個資保護，依 GDPR 規定，在對兒少提供資訊社會服務（Information Society Services，指依當事人要求而以遠距電子方式提供資訊並收取費用之服務，例如影音串流、互動數位電視），並以「個資當事人同意」作為處理個資之法律依據的情況下，該兒少須年滿 16 歲，其同意始為合法；對於未滿 16 歲之兒少，僅限於其法定代理人給予或授權同意之範圍內，始得合法處理其個人資料。不過歐盟各會員國得以法律降低前述 16 歲的門檻，但不得低於 13 歲[25]。

又控管者有義務以合理的努力，考量現有之科技，確認前述法定代理人給予或授權同意[26]。

[25] GDPR, Article8(1), "Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

[26] GDPR, Article8(2), "The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology."

7、當事人權利

GDPR 賦予個資當事人下列權利，以提升個資當事人的自主控制權並促進個人資料保護：

7.1 資訊近用（access）權

個資當事人有權向控管者確認其個資是否正被處理，如有，個資當事人有權近用其個資及下列資訊[27]：

- 個資處理之目的；
- 所涉個人資料之類別；
- 已提供或擬提供個資之個資接受者身分或類別，特別是在第三國或國際組織之個資接受者。

[27] GDPR, Article15(1), "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: a) the purposes of the processing; b) the categories of personal data concerned; c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

- 如可能時，個人資料將被儲存之預期期間，或如不可能告知期間者，決定個資儲存期間之標準。
- 向控管者請求更正、刪除或限制處理、反對處理個資之權利。
- 向監管機關提起申訴之權利。
- 個資不是向個資當事人蒐集者，關於個資來源之任何可得資訊；
- 控管者採取之自動化決定行為及作成該決定所採邏輯之有意義資訊，以及該處理個資行為之重要性與預期結果。
- 如個人資料傳輸至第三國或國際組織，個資當事人有權獲知與該傳輸有關的適當安全維護措施[28]。

7.2 更正權

個資當事人有權請求控管者即時更正不正確之個人資料，且考量處理個資之目的，個資當事人有權請求補充其個人資料[29]。

[28] GDPR, Article15(2), "Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer."

[29] GDPR, Article16, "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

7.3 刪除權

有下列情形之一時，個資當事人原則上有權請求控管者即時刪除其個人資料[30]：

- 個人資料對於原本蒐集或處理之目的已無必要。
- 個資當事人撤回同意，且無其他法律依據。
- 個資當事人依 GDPR 規定對處理個資行為表示反對。
- 個人資料遭違法處理。
- 控管者依法律規定有義務刪除個人資料。
- 控管者對兒少提供資訊社會服務。

7.4 被遺忘權

如控管者已將個人資料公開，且依據上述規定有義務刪除該個人資料時，該控管者應考量現有科技及執行成本，採取合理步驟（包括以技術性方式）將個資當事人已提出刪除其個人資料之

[30] GDPR, Article17(1), "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

任何連結、副本或複製本（檔）的請求，通知正在處理該個人資料之控管者[31]。

7.5 限制處理權

有下列情形之一時，個資當事人有權限制控管者處理其個人資料[32]：

- 個資當事人質疑個人資料之正確性，並給予控管者驗證該個人資料正確性之期間。
- 控管者違法處理個人資料，但個資當事人拒絕刪除個資而要求限制使用個資。
- 控管者依其處理之目的已不再需要該個人資料，但該個人資料是個資當事人建立、行使或防禦法律上請求所必須者。

[31] GDPR, Article17(2), "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. "

[32] GDPR, Article18(1), "The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject."

- 個資當事人依 GDPR 規定反對處理其個資，並尚待確認控管者是否具有優於個資當事人利益的正當理由。

7.6 個資可攜權

更多個資可攜權資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on the right to data portability》。連結見《參考資源》

在符合下列兩項前提下，個資當事人有權對其提供給控管者的個人資料取得一份具備「結構化」、「普遍使用」、「機器可讀」之格式的檔案，並有權將該個資檔案移轉給另一控管者而不受原本控管者之阻礙[33]：

- 控管者處理個資之法律依據為「當事人同意」或「與當事人有契約（前）關係」。
- 控管者以自動化方式處理個資。

個資當事人行使個資可攜權時，如技術許可，應有權要求將其個資檔案直接自原本控管者移轉至另一控管者[34]。

[33] GDPR, Article20(1), "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and b) the processing is carried out by automated means."

[34] GDPR, Article20(2), "In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."

7.7 反對處理權

如控管者處理個資之法律依據為「基於公共利益」或「基於正當利益」時，個資當事人有權依具體情形，隨時反對控管者處理其個人資料，包含對個資當事人作出剖析（profiling）。此時控管者即不得再處理其個人資料，除非能證明處理其個資有優於個資當事人利益、權利及自由之正當理由，或是為了建立、行使或防禦法律上請求[35]。

又如控管者是為直接行銷之目的而處理個人資料時，該個資當事人有權隨時反對為行銷而處理其個資，包括反對與該直接行銷有關範圍內之剖析。此時控管者即不得再為行銷目的而處理其個人資料[36]。

[35] GDPR, Article21(1), "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."

[36] GDPR, Article21(2), "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing."

更多自動化決定資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679》。連結見《參考資源》

7.8 免於自動化決定權

個資當事人有權不受控管者僅透過自動化處理個資（包含剖析）之方式，對其作出具有法律效果或類似重要影響之決定[37]，除非有下列情形之一[38]：

- 該決定是為締結或履行個資當事人與控管者間之契約所必須。
- 該決定是法律許可且該法律訂有適當措施以維護個資當事人的權利、自由及正當利益。
- 該決定是基於個資當事人的明確同意。

但如控管者基於「為締結或履行個資當事人與控管者間之契約所必須」或「個資當事人的明確同意」之理由作成前述決定時，

[37] GDPR, Article22(1), "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

[38] GDPR, Article22(2), "Paragraph 1 shall not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) is based on the data subject's explicit consent."

控管者應採取適當措施保護個資當事人的權利、自由及正當利益，至少使個資當事人有權獲得控管者的人為參與，以表達意見並質疑該決定[39]。

[39] GDPR, Article22(3), "In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

更多告知義務（透明性）資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on transparency under Regulation 2016/679》。連結見《參考資源》

8、告知義務

控管者有義務對個資當事人以下列形式及內容，提供必要法定資訊：

8.1 告知之形式要件

控管者應通過適當方式，以簡明、透明、易懂且方便取得之格式，採用清楚簡易之語言，將法定資訊提供予個資當事人。該資訊應以書面或其他方式提供，包括於適當情況下之電子格式。惟如當個資當事人提出要求，並得以其他方式確認個資當事人身分者，得以口頭提供該等資訊[40]。

[40] GDPR, Article12(1)," The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means."

控管者提供前述資訊時，得以標準化之圖示方式提供，俾以易見、易懂且清晰易讀之方式，對於所欲進行之處理提供有意義之概述。如該等圖示係以電子方式呈現，應為機器可讀之形式[41]。

8.2 告知之實質內容

依 GDPR 第 13 條關於「直接取得」個人資料[42]及第 14 條關於「間接取得」個人資料[43]的規定，控管者應提供下列資訊予個資當事人：

[41] GDPR, Article12(7), "The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable."

[42] GDPR, Article13(1), "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: a) the identity and the contact details of the controller and, where applicable, of the controller' s representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; e) the recipients or categories of recipients of the personal data, if any; f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

[43] GDPR, Article14(1), "Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: a) the identity and the contact details of the controller and, where applicable, of the controller' s representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) the categories of personal data concerned; e) the recipients or categories of recipients of the personal data, if any; f) where applicable, that the controller intends to transfer personal data to a recipient in

- 控管者的身分、聯絡資訊與個資保護長。
- 處理個資之目的及法律依據。
- 控管者或第三人處理個資的正當利益（如有）。
- 個資種類（僅間接蒐集須告知）。
- 接受個資之第三人或其類別。
- 跨境傳輸個資之細節與安全維護措施。
- 保存期間或決定保存期間之條件。
- 個資當事人得行使的各項權利。
- 在相關事項中個資當事人得隨時撤回同意。
- 取得個資之來源及是否來自公開資料（僅間接蒐集須告知）。
- 個資當事人是否有義務提供個資及不提供個資將可能造成的影響（僅直接蒐集須告知）。
- 是否存在以自動化方式對個資當事人作出決定的情形，包含剖析（profiling），以及如何作出決定及其重要性與影響。

---

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

9、控管者責任

為了強化個人資料保護，GDPR 對控管者設有若干具體行為規範，要求控管者承擔責任：

9.1 舉證與記錄

控管者應負擔遵守各項處理個資原則（合法性、公平性、透明性、目的限制、資料最小化、正確性、儲存限制、完整性、機密性）之責，並應對此負舉證責任[44]。

又控管者應考量處理個資行為的性質、內容、範圍、目的及對個資當事人之權利與自由的不同風險可能性和嚴重性，採取適當的技術上及組織上措施以確保遵守 GDPR 的各種規範，且亦應負舉證之責[45]。

此外，控管者（及其歐盟境內之代理人）應以文件（包含電子文件[46]）記錄下列資訊[47]，且應依監督機關之要求而提出[48]：

---

[44] GDPR, Article5(2), "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

[45] GDPR, Article24(1), "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

[46] GDPR, Article30(3), "The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form."

[47] GDPR, Article30(1), "Each controller and, where applicable, the controller' s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: a) the name and contact details of the controller and, where applicable, the joint controller, the controller' s

- 控管者及共同控管者、代理人、個資保護長(如有)之名稱(姓名)與聯絡資訊。
- 處理個資之目的。
- 個資當事人類別及個資類別的描述。
- 曾經或將會揭露個資的對象類別，包含位於第三國或國際組織的接受者。
- 將個資傳輸至第三國或國際組織之情形，包含該第三國或國際組織之身分及控管者採取適當安全維護之記錄。
- 預設刪除不同類別個資之期限。
- 所採取技術上及組織上之安全維護措施的概述。

不過，如控管者的員工少於 250 人，即可免於上述記錄資訊的義務，除非[49]：

---

representative and the data protection officer; b) the purposes of the processing; c) a description of the categories of data subjects and of the categories of personal data; d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; f) where possible, the envisaged time limits for erasure of the different categories of data; g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."

[48] GDPR, Article30(4), "The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request."

[49] GDPR, Article30(5), "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the

- 處理個資行為對個資當事人的權利與自由有可能產生風險。
- 該處理個資行為非偶發性。
- 該處理個資行為涉及特種個資或刑事個資。

9.2 個資保護設計 / 個資保護預設

依 GDPR 規定，考量當下技術水平、費用及處理個資行為的性質、範圍、內容、目的及對自然人的權利與利益之不同風險可能性和嚴重性，控管者在事前決定處理個資之方法及處理個資時，應採取適當的技術上及組織上措施以有效導入各項個資保護原則，例如以匿名化方式達成個資最小化原則(data minimisation)，並將必要的安全維護措施整合進入處理個資的行為中，以滿足 GDPR 的要求且保護個資當事人的權利[50]。

又控管者應採取適當的技術上與組織上措施以確保處理個資行為之預設模式為「僅處理為達成個別蒐集目的之必要個資」，

processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

[50] GDPR, Article25(1), "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

此義務適用於蒐集個資的數量、處理個資的範圍、儲存與存取個資的期間等，尤其應預設防止個人資料在未得當事人意思表示的情況下遭不特定人存取[51]。

更多個資保護衝擊評估資訊，請參歐盟第 29 條個資保護工作小組(Article 29 Data Protection Working Party) 發布《Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679》。連結見《參考資源》

9.3 個資保護衝擊評估與事前諮詢

9.3.1 執行評估的條件

依 GDPR 第 35 條第 1 項規定[52]，控管者如考量其處理個資行為的性質、範圍、內容及目的，尤其是「以新興科技處理個資」的情況，將對自然人的權利與自由產生「造成高度風險的可能性」時，應在處理個資前，針對擬處理個資之行為將對

[51] GDPR, Article25(2), "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual' s intervention to an indefinite number of natural persons."

[52] GDPR, Article35(1), "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

個資保護帶來的衝擊執行評估（Data Protection Impact Assessments，DPIA）。

GDPR 第 35 條第 3 項更補充規定[53]，要求如有下列情況之一者，即應執行評估：

- 以自動化方式（包含剖析，即對個人資料任何形式之自動化處理，包括使用個人資料來評估與特定人有關之個人特徵，特別是用來分析或預測有關該自然人之工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、位置或動向等特徵 ）而系統性及廣泛性對自然人進行評估（evaluation），並依此對該自然人作出法律上或相似重要影響之決定。
- 大規模處理特種個資或刑案資料。
- 對公開場所進行大規模的系統性監控。

9.3.2 評估之內容

個資保護衝擊評估之內容至少應包含下列事項[54]：

[53] GDPR, Article35(3), "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: a) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or c) a systematic monitoring of a publicly accessible area on a large scale."

[54] GDPR, Article35(7), "The assessment shall contain at least: a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) an assessment

- 對預定處理個資之行為及目的做系統性描述，包含控管者處理個資的正當利益。
- 評估該處理個資行為對處理目的之必要性與合比例性。
- 評估對個資當事人之權利與自由可能造成的風險。
- 預定因應風險的措施。

9.3.3 事前諮詢

如個資保護衝擊評估顯示，處理個資行為因控管者未採取降低風險的措施而將導致高度風險時，控管者應於處理個資前事先諮詢監督機關[55]。

9.4 指派個資保護長

更多個資保護長資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on Data Protection Officers》。 連結見《參考資源》

of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

[55] GDPR, Article36(1), "The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

9.4.1 指派個資保護長的條件

依 GDPR 第 37 條第 1 項規定[56] ，符合下列三種情況之一的控管者，即應指派「個資保護長(Data Protection Officers，DPO)」：

- 公務機關處理個資。
- 核心業務即為處理個資，且該處理個資行為需對個資當事人進行大規模的常態性及系統性監控。
- 核心業務為大規模的處理特種個資或刑案個資。

9.4.2 個資保護長的任務

依 GDPR 第 39 條第 1 項規定[57]，個資保護長的任務應至少包含下列項目：

---

[56] GDPR, Article37(1), "The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

[57] GDPR, Article39(1), "The data protection officer shall have at least the following tasks: a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; c) to provide advice where requested as regards the data protection impact assessment and monitor its

- 向控管者及其執行處理個資行為之受雇人告知在 GDPR 和其他歐盟或會員國法律下的義務，並提出建議。
- 監督控管者在個資保護方面是否遵循 GDPR、其他歐盟或會員國法律或機關內部政策，包含責任分配、認知提升、員工訓練及稽核等。
- 在控管者為執行個資保護衝擊評估而向個資保護長諮詢時提供建議，並監督其執行。
- 與主管機關合作。
- 作為主管機關對於處理個資有關事項的聯絡對象。

9.4.3 個資保護長的專業能力

為能有效執行任務，GDPR 第 37 條第 5 項規定[58]，個資保護長應具備專業能力，尤其是個資保護法律與實務的專家知識。

performance pursuant to Article 35; d) to cooperate with the supervisory authority; e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."

[58] GDPR, Article37(5), "The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39."

9.4.4 個資保護長的地位

依 GDPR 第 38 條第 2 項規定[59]，控管者應提供個資保護長必要資源、讓其接觸個資處理業務及維持專業知識，以便執行任務。

9.4.5 個資保護長的獨立性

GDPR 第 38 條第 3 項[60]及第 6 項[61]以下列規定保障個資保護長的獨立性，以使其能有效執行任務：

- 個資保護長於執行任務時不受控管者的任何指示。
- 個資保護長不因執行任務之行為而遭免職或罰款。
- 個資保護長應直接向控管者的最高管理階層彙報。
- 個資保護長雖得執行其他任務或履行其他義務，但控管者應確保該任務或義務不得與個資保護長之職位有利益衝突。

---

[59] GDPR, Article38(2), "The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge."

[60] GDPR, Article38(3), "The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor."

[61] GDPR, Article38(6), "The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."

10、處理者規定

10.1 處理者資格

控管者僅得委託足以保證採取適當之技術上及組織上措施以符合 GDPR 要求並確保個資當事人權利保護的處理者，指示其處理個人資料[62]。

10.2 控管者約束

控管者應以雙方間的契約或其他歐盟或會員國法律下的法律行為約束處理者處理個資的行為，並約定委託處理個資之主要內容、期間、性質、目的、個資種類、當事人類別及控管者的權利與義務。該契約或其他法律行為應以書面為之（包含電子文件形式）[63]，並應約定處理者有下列義務[64]：

---

[62] GDPR, Article28(1), "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

[63] GDPR, Article28(9), "The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form."

[64] GDPR, Article28(3), "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. 2That contract or other legal act shall stipulate, in particular, that the processor: a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on

- 僅依控管者的書面指示處理個資，包含將個人資料傳輸至第三國或國際組織，除非處理者係受歐盟或會員國法律要求為之；在此情況下，處理者應在處理個資前將該法律要求通知控管者，除非該法律以維護重要公益之理由禁止之。
- 確保經授權處理個資之人承諾保密或受其他適當的保密義務拘束。
- 採取 GDPR 要求的適當安全維護措施。
- 遵守複委託的條件（見下 10.3）。
- 考量處理個資行為之性質，在可能的範圍內以適當之技術上及組織上措施，協助控管者履行控管者回應個資當事人行使權利的義務。

---

important grounds of public interest; b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; c) takes all measures required pursuant to Article 32; d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller' s obligation to respond to requests for exercising the data subject' s rights laid down in Chapter III; f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

- 考量處理個資行為之性質及處理者掌握之資訊，協助控管者確保遵循 GDPR 關於安全維護、個資侵害事故通報與通知、個資保護衝擊評估與事前諮詢等義務。
- 依控管者的選擇，於處理個資之服務終止後，刪除所有個資或返還控管者，並刪除現存的複本。但歐盟或會員國法律要求儲存個資者，不在此限。
- 供控管者取得所有得以證明處理者遵守義務之資訊，並允許及促成控管者或其指定之稽核員執行稽核，包含實地視察。

10.3 複委託條件

除非控管者事先以書面授權 (個案或概括)，否則處理者不得將受託事項複委託第三人。在控管者概括授權的情況，處理者應將任何有關增加或變更複委託第三人的情事通知控管者，以提供控管者得拒絕的機會[65]。

如處理者複委託第三人時，該第三人應依契約或其他法律行為而受個資保護義務的拘束，尤其是保證採取適當之技術上

[65] GDPR, Article28(2), "The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

及組織上措施以符合 GDPR 要求。若該第三人未能遵守個資保護義務，處理者應就其行為對控管者承擔全部責任[66]。

10.4 處理者的記錄義務

處理者（及其歐盟境內之代理人）應以文件（包含電子文件[67]）記錄下列資訊[68]，且應依監督機關之要求而提出[69]：

- 處理者（及其歐盟境內之代理人）與個別控管者（及其歐盟境內之代理人）及各自之個資保護長（如有）的名稱（姓名）及聯絡資訊。

---

[66] GDPR, Article28(4), " Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

[67] GDPR, Article30(3), "The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form."

[68] GDPR, Article30(2), "Each processor and, where applicable, the processor' s representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller' s or the processor' s representative, and the data protection officer; b) the categories of processing carried out on behalf of each controller; c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."

[69] GDPR, Article30(4), "The controller or the processor and, where applicable, the controller' s or the processor' s representative, shall make the record available to the supervisory authority on request."

- 控管者指示處理個資的類別。
- 將個資傳輸至第三國或國際組織之情形，包含該第三國或國際組織之身分及採取適當安全維護之記錄。
- 對於所採取技術上與組織上的安全維護措施之概述。

但與控管者相同，如處理者的員工少於 250 人，即可免於上述記錄資訊的義務，除非[70]：

- 處理個資行為對個資當事人的權利與自由有可能產生風險。
- 該處理個資行為非偶發性。
- 該處理個資行為涉及特種個資或刑事個資。

10.5 指派個資保護長

前述 GDPR 關於指派個資保護長的規定，對處理者也有適用，即處理者在符合特定條件下，也有指派個資保護長的義務。

[70] GDPR, Article30(5), "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

更多個資侵害事故通報與通知資訊，請參歐盟第 29 條個資保護工作小組（Article 29 Data Protection Working Party）發布《Guidelines on Personal data breach notification under Regulation 2016/679》。連結見《參考資源》

11、個資侵害事故通報與通知

11.1 向監督機關通報

個資侵害事故發生時，除非該事故不至於對自然人的權利與自由產生風險，否則控管者在可行的情況下，應於知悉事故發生後 72 小時內通報主管監督機關；如有遲延並應附理由[71]。而處理者在知悉個資侵害事故後，應即時通知控管者[72]。

控管者向主管監督機關通報個資侵害事故之內容應至少包含下列事項[73]：

[71] GDPR, Article33(1), "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

[72] GDPR, Article33(2), "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

[73] GDPR, Article33(3), "The notification referred to in paragraph 1 shall at least: a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c) describe the likely consequences of the personal

- 描述個資事故的性質，包含在可能的情況下描述個資當事人的類別與大約數量，及個資檔案的類別及大約數量。
- 告知個資保護長或其他聯絡人的姓名及聯絡資訊，以供獲得更多資訊。
- 描述該個資侵害事故可能造成的後果。
- 描述控管者已採取或將採取對應該侵害事故的措施，如適當時，應包含降底損害的措施。

又控管者應紀錄任何個資侵害事故，包含與事故有關之事實、影響及補救措施。該紀錄應使監管機關得以查核是否遵循 GDPR 之相關規定[74]。

11.2 向個資當事人通知

如該個資侵害事故將可能對自然人的權利與自由產生高度風險時，控管者應即時向個資當事人通知該個資侵害事故[75]，但有下列情形之一時，控管者可無須通知個資當事人[76]：

---

data breach; d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

[74] GDPR, Article33(5), "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

[75] GDPR, Article34(1), "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

- 控管者已導入適當之技術上與組織上保護措施，且該措施即應用於該次個資侵害事故影響之個人資料，尤其是使個人資料讓任何未獲授權而取得之人無法理解之措施，例如加密。
- 控管者已採取後續措施以確保對個資當事人之權利與自由具有之高度風險已不再可能實現。
- 通知將付出不合比例的成本。在此情況下，應以公告或其他個資當事人得以相同有效方式獲得通知之類似方法代替。

控管者向個資當事人通知個資侵害事故之內容，應以清楚、簡白之語言描述個資侵害事故的性質，且應至少包含下列資訊與措施[77]：

- 告知個資保護長或其他聯絡人的姓名及聯絡資訊，以供獲得更多資訊。

---

[76] GDPR, Article34(3), "The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

[77] GDPR, Article34(2), "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."

- 描述該個資侵害事故可能造成的後果。
- 描述控管者已採取或將採取對應該侵害事故的措施，如適當時，應包含降低損害的措施。

12、跨境傳輸個人資料

我國個人資料保護法對於個資之跨境傳輸採「原則許可、例外限制」之規範方式，此與 GDPR 採「原則禁止、例外許可」大不相同，且由於跨境傳輸之違反可能導致 GDPR 第 83 條第 5 項之處罰（即 2000 萬歐元或年度全球營收 4%），因此我國企業、組織需審慎評估是否合於 GDPR 跨境傳輸之規範。

12.1 跨境傳輸個資的條件

GDPR 規定，必須符合下列情況之一，才可將個人資料傳輸至歐盟境外的第三國或國際組織：

- 第三國或國際組織具備歐盟認定的個資保護適足性[78]，但我國目前尚未符合此要件。
- 但作為控管者或處理者的台灣企業、組織，仍可採取適當安全維護措施，並確保個資當事人行使權利及法律救濟的有效性[79]，而可跨境傳輸個人資料，例如[80]：

[78] GDPR, Article45(1), "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."

[79] GDPR, Article46(1), "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

- 個資傳輸者與個資接受者間存有 GDPR 第 47 條規定的約束性企業規則（binding corporate rules）。
- 個資傳輸者與個資接受者間簽訂標準個資保護條款（standard data protection clauses）。
- 個資接受者依具有拘束性與執行性之承諾，遵守歐盟認可的行為守則（code of conduct）而採取適當安全維護措施。
- 個資接受者取得歐盟認可的認證（certification），並依具有拘束性與執行性之承諾而採取適當安全維護措施。

- 如果不具備適足性，也未能採取有效的適當安全維護措施時，便只能在下列情形跨境傳輸個人資料，重點包含[81]：

---

[80] GDPR, Article46(2), "The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a) a legally binding and enforceable instrument between public authorities or bodies; b) binding corporate rules in accordance with Article 47; c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."

[81] GDPR, Article49(1), "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: a) the data

- 個資當事人經告知如個資傳輸至該不具備適足性且無適當安全維護之第三國或國際組織所可能帶來的風險後，明確表示同意。
- 該傳輸係為履行個資當事人與控管者間之契約所必要，或是應當事人的要求，為締結契約之準備行為所必要。
- 該傳輸係為重大公共利益所必要。

13、處罰

GDPR 依控管者或處理者的違法情形，區分兩種等級的行政處罰，且 GDPR 之行政處罰金額遠較我國個人資料保護法規定為高，因此我國企業、組織需特別留意。

---

subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject' s request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case."

13.1 最高可處 1 千萬歐元或該會計年度的全球營收 2%（取較高者）的行政罰鍰，例如[82]：

- 未取得未滿 16 歲兒少之法定代理人的（授權）同意而蒐集兒少個資（GDPR 第 8 條）。
- 控管者依其蒐集個資之目的不需或已不再需要識別當事人之身分，卻仍繼續保存、取得或處理可識別當事人的資料（GDPR 第 11 條）。
- 控管者或處理者違反 GDPR 第 4 章第 25 條至第 39 條規範之義務，例如：記錄處理個資資訊、預設個資保護、執行個資保護衝擊評估、指派個資保護長等。

13.2 最高可處 2 千萬歐元或該會計年度的全球營收 4%（取較高者）的行政罰鍰，例如[83]：

[82] GDPR, Article83(4), "Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; b) the obligations of the certification body pursuant to Articles 42 and 43; c) the obligations of the monitoring body pursuant to Article 41(4)."

[83] GDPR, Article83(5), "Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; b) the data subjects' rights pursuant to Articles 12 to 22; c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; d) any obligations pursuant to Member State law adopted under Chapter IX; e) non-compliance with an order or a temporary or definitive limitation on processing or

- 控管者或處理者違反 GDPR 第 2 章的個資處理原則。
- 侵害個資當事人依 GDPR 第 3 章享有之權利。
- 違反 GDPR 第 5 章關於跨境傳輸個人資料之規定。
- 未遵守主管機關作出的命令或限制，或未提供主管機關執行行政檢查時存取資料之權限。

the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)."

參考資源

1. 歐盟：Article 29 Data Protection Working Party, 《EU GENERAL DATA PROTECTION－GENERAL INFORMATION DOCUMENT》。
   https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiKuIzRrYTbAhXFo5QKHbQaDigQFggoMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Fdoc_id%3D49751&usg=AOvVaw2278bkbEk704p95swHvcGB
   最後到訪日為 107 年 5 月 14 日。
2. 歐盟：Article 29 Data Protection Working Party,《Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC》, wp214。
   http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
   最後到訪日為 107 年 5 月 14 日。
3. 歐盟：Article 29 Data Protection Working Party,《Guidelines on the right to "data portability"》, wp242rev.01。
   http://ec.europa.eu/newsroom/document.cfm?doc_id=44099
   最後到訪日為 107 年 5 月 14 日。
4. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Data Protection Officers ('DPOs')》, wp243rev.01。
   http://ec.europa.eu/newsroom/document.cfm?doc_id=44100
   最後到訪日為 107 年 5 月 14 日。

5. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Data Protection Impact Assessment (DPIA)》, wp248rev.01。
http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
最後到訪日為 107 年 5 月 14 日。
6. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Personal data breach notification under Regulation 2016/679》, wp250rev.01。
http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827
最後到訪日為 107 年 5 月 14 日。
7. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679》, wp251rev.01。
http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826
最後到訪日為 107 年 5 月 14 日。
8. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Consent under Regulation 2016/679》, wp259rev.01。
http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030
最後到訪日為 107 年 5 月 14 日。
9. 歐盟：Article 29 Data Protection Working Party,《Guidelines on Transparency under Regulation 2016/679》, wp260rev.01。
http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

最後到訪日為 107 年 5 月 14 日。