ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN

WP 243 rev.01

Guidelines on Data Protection Officers ('DPOs')
關於個資保護長（DPO）之指引

Adopted on 13 December 2016

As last Revised and Adopted on 5 April 2017

2016年12月13日通過

2017年4月5日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 05/35.
由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
網址：http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

關於個人資料運用*之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,
having regard to Articles 29 and 30 thereof,
having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日之第95/46/EC號指令而設立，
基於該指令第29條及第30條，
基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:

通過此份指引：

＊譯註：我國個資法將個資之使用分為蒐集(collection)、處理(processing)、利用(use)等不同行為態樣，且有相應之適用要件，而GDPR對個資之蒐集、處理、利用任一行為，皆統稱為 processing。為與我國個資法中之「處理」有所區隔，本文因此將GDPR中的processing 譯為「運用」，processor 譯為「受託運用者」。

Table of content

目錄

1 Introduction 導言

The General Data Protection Regulation ('GDPR'),[1] due to come into effect on 25 May 2018, provides a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR.

訂於2018年5月25生效之「一般資料保護規則（General Data Protection Regulation，GDPR）」[1]提供了歐洲一套現代化、以課責性為基礎之資料保護遵循架構。個資保護長（DPO）將會是此一新法律架構下，許多組織中推動遵循GDPR規範之核心。

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO.2 This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

於GDPR規範下，對某些控管者及受託運用者而言，必須指派一名DPO[2]。此規範適用於所有公務機關或機構（無論其運用何種資料），及其他核心業務為大規模對個人進行系統性監控，或大規模運用特種個人資料之組織。

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

即使在GDPR未明確要求必須指派DPO之情況下，各組織有時也可能認為設置DPO有其

[1] 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), (OJ L 119, 4.5.2016). The GDPR is relevant for the EEA and will apply after its incorporation into the EEA Agreement.

2016年4月27日歐洲議會與歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，並廢除第95/46/EC號指令，制定歐盟第2016/679號規則（一般資料保護規則）（OJ L 119, 4.5.2016）。GDPR與歐洲經濟區相關，並將在納入歐洲經濟區協議後適用。

[2] The appointment of a DPO is also mandatory for competent authorities under Article 32 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89 – 131), and national implementing legislation. While these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions.

歐洲議會與歐盟理事會2016年4月27日通過之歐盟第2016/680號指令第32條，係權責機關為預防、調查、發現或起訴犯罪或執行刑罰之目的所為個資運用中對自然人之保護、確保該資料自由流通，並廢除理事會第2008/977/JHA號架構決定（OJ L 119, 4.5.2016, p. 89 – 131），以及各國之執行法規，主管機關指派DPO亦為強制規定。此指導原則雖聚焦於GDPR下規範之DPO，但亦可為第2016/680號指令中，近似條文規範DPO事宜之參照。

益處而自願指派。第29條資料保護工作小組（下稱WP29）亦鼓勵此自願性質之努力。

The concept of DPO is not new. Although Directive 95/46/EC [3] did not require any organisation to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years.
DPO並非新的概念。95/46/EC指令[3]雖未要求任何組織須指定DPO，但此種指派DPO之作法已於若干會員國發展多年。

Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.[4] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).
於GDPR通過前，WP29即主張DPO為課責性之基石，且指定DPO可促進法遵，並進一步成為企業之競爭優勢[4]。除透過採用課責性工具（如推動個資保護影響評估及實施或推動稽核作業）促進法遵外，DPO亦為相關利害關係人（例如：監管機關、當事人及組織內之業務單位）間之中介者。

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.
如未遵循GDPR，並不歸責於DPO個人。GDPR清楚規定應由控管者或受託運用者確保並得以證明依其規範執行運用（第24條第1項）。遵循資料保護規範，係控管者或受託運用者之責任。

The controller or the processor also has a crucial role in enabling the effective performance of

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).
1995年10月24日歐洲議會與歐盟理事會在個人資料運用上為保護自然人與確保該資料之自由流通，所制定之歐盟第95/46/EC號指令（OJ L 281, 23.11.1995, p. 31）。
[4] See http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf
詳參 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively.
控管者或受託運用者於使DPO有效執行任務上，亦扮演重要角色。指定DPO僅是第一步，DPO亦須被賦予充足之自主性及資源方可有效執行任務。

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of these guidelines is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States. The WP29 will monitor the implementation of these guidelines and may complement them with further details as appropriate.
GDPR將DPO視為嶄新的資料治理體系中之關鍵角色，並規定了DPO指派之條件，及其職位與任務。本指引之目的在於釐清GDPR之相關條文，以協助控管者及受託運用者遵循該法，亦在於協助DPO扮演其角色。本指引亦以部分歐盟成員國之經驗為基礎，就最佳做法提出建議。WP29將持續留意此指引之執行情形，並可能於後續適時補充更多細節。

2 Designation of a DPO
DPO之指派

2.1. Mandatory designation
強制指派

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:[5]
GDPR第37條第1項要求在三種情形下必須指派DPO[5]：

a) where the processing is carried out by a public authority or body;[6]
資料運用係由公務機關或機構為之；[6]

b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or

[5] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well.
此處應留意，依據第37條第4項規定，歐盟或會員國法律可能要求於其他情形下，亦須指派DPO。
[6] Except for courts acting in their judicial capacity. See Article 32 of Directive (EU) 2016/680.
除法院行使其司法功能外。參照歐盟第2016/680號指令第32條。

控管者或受託運用者之核心業務，包含需經常性、系統性對當事人進行大規模監控之運用作業；或

c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data[7] or[8] personal data relating to criminal convictions and offences.[9]
控管者或受託運用者之核心業務，包含大規模運用特種資料[7]或[8]與刑事前科及犯罪相關之個人資料[9]。

In the following subsections, the WP29 provides guidance with regard to the criteria and terminology used in Article 37(1).
WP29於以下小節就第37條第1項之標準及術語提供指導。

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.[10] This analysis is part of the documentation under the accountability principle. It may be required by the supervisory authority and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services that might fall within the cases listed in Article 37(1).
除組織顯無須指派DPO外，WP29建議控管者及受託運用者記錄其決定是否要指派DPO所進行之內部分析，以證明相關因素均已妥善納入考量[10]。此分析為課責性原則下證明文件之一部分。監管機關可能會要求提供該項分析，必要時並應更新該項分析，例如控管者或受託運用者從事之新業務或提供之新服務可能落入第37條第1項所列情形時。

When an organisation designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been

[7] Pursuant to Article 9 these include 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.
依據第9條規定，此類別包括種族或民族血統、政治觀點、宗教或哲學信仰、公會會員資格、為識別自然人而運用之基因資料及生物辨識資料、健康相關資料或自然人之性生活或性傾向相關資料。
[8] Article 37(1)(c) uses the word '*and*'. See Section 2.1.5 below for explanation on the use of '*or*' instead of '*and.*'
第37條第1項第c款之用字為「及」。參照本指引第2.1.5節以下關於使用「或」而不用「及」之說明。
[9] Article 10.
第10條。
[10] See Article 24(1).
參照第24條第1項。

mandatory.

當一組織自願指派DPO時，其指派、職位及任務即與強制指派同樣適用第37條至第39條之要件。

Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data. In this case it is important to ensure that there is no confusion regarding their title, status, position and tasks. Therefore, it should be made clear, in any communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a data protection officer (DPO). [11]

法律上無義務也無意自願指派DPO之組織，由其員工或外部顧問執行個資保護之相關任務，亦無不可。在此情形下，重要的是確保該人員之職稱、地位、職位及任務不得混淆。因此，於公司內部及其與資料保護機關、當事人及一般大眾間之溝通中，該員或顧問的職稱不得為DPO[11]。

The DPO, whether mandatory or voluntary, is designated for all the processing operations carried out by the controller or the processor.

無論強制或自願性指派之DPO，係為控管者或受託運用者所有的資料運用作業而指派。

2.1.1 'PUBLIC AUTHORITY OR BODY'

公務機關或機構

The GDPR does not define what constitutes a '*public authority or body*'. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[12] In such cases, the designation of a DPO is mandatory.

[11] This is also relevant for chief privacy officers ('CPO's) or other privacy professionals already in place today in some companies, who may not always meet the GDPR criteria, for instance, in terms of available resources or guarantees for independence, and, if they do not, they cannot be considered and referred to as DPOs.
此規定亦涉及首席隱私長（chief privacy officers，CPO）或其他目前在部分公司中已存在之隱私專業人員。該人員可能不完全符合GDPR規定之相關條件（例如可利用之資源或獨立性之保障），倘不符合，即不能將其視為DPO或以DPO稱之。

[12] See, e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of 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).
「*公務機構*」及「*受公法管轄之機構*」之定義，可參照2003年11月17日歐洲議會與歐盟理事會為公部門資訊再利用制定之第2003/98/EC號指令第2條第1項及第2項。

GDPR對何謂「*公務機關或機構*」並無定義。WP29認為此一概念應由國內法決定。因此，公務機關與機構包括國家、區域及地方之機關，但此概念於國內法適用上一般也包括部分受公法管轄之其他機構[12]。於此情形下，DPO之指派為強制性。

A public task may be carried out, and public authority may be exercised[13] not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.

公共事務之執行及公權力之行使，除可能由公務機關或機構為之外，依據各會員國之國內法，也可能由受公法或私法管轄之自然人或法人行使，如大眾運輸服務、水及能源供應服務、道路基礎設施、公共廣播服務、公共住宅或法定專業人士之紀律組織等[13]。

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.

於此情形，當事人所處之情境與其資料由公務機關或機構運用之情境可能甚為相似。特別是在資料運用目的相似，且個人通常同樣對於其資料是否被運用與如何運用之選擇性甚低，或無法選擇，因此需要指派DPO給予額外保護。

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO. Such a DPO's activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

於此情形，執行公共事務或行使公權力之私人組織雖無指派DPO之義務，WP29仍建議其指派DPO為優良作法。此種DPO之業務涵蓋所有資料運用作業，包含那些與公共事務執行及公權力行使無關（如員工資料庫管理）之作業。

2.1.2 'CORE ACTIVITIES'

核心業務

[13] Article 6(1)(e).
第6條第1項第e款。

Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor'*. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.

GDPR第37第1項第b款及c款提及「*控管者或受託運用者之核心業務*」。前言第97點明確指出，控管者之核心業務係「*與主要業務相關，與運用個資之附屬業務無關者*」。可將「核心業務」視為達成控管者或受託運用者目標之必要關鍵作業。

However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.

然而，當運用資料為控管者或受託運用者業務中所不可分割之一部分時，運用資料不應被解釋為排除在「核心業務」範圍之外。例如，醫院之核心業務為提供醫療保健。然而，醫院如不運用健康資料(如病患之健康紀錄)，即無法安全有效地提供醫療保健服務。因此，運用這些資料應視為每所醫院核心業務之一，故醫院必須指派DPO。

As another example, a private security company carries out the surveillance of a number of private shopping centres and public spaces. Surveillance is the core activity of the company, which in turn is inextricably linked to the processing of personal data. Therefore, this company must also designate a DPO.

另一個例子是，私人保全公司會對若干購物中心及公共空間進行監視。此監視工作係該公司之核心業務，亦無可避免需連結至個資運用作業。因此，此公司必須指派DPO。

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

另一方面，有些業務是所有組織均會執行的，如支付員工薪資，或一般資訊科技支援工作。這些例子乃組織核心業務或主要經營領域所必須具備之支援功能。即使此業務係必需或必要，一般仍視為附屬功能而非核心業務。

2.1.3 'LARGE SCALE'
大規模

Article 37(1)(b) and (c) requires that the processing of personal data be carried out on a large scale in order for the designation of a DPO to be triggered. The GDPR does not define what constitutes large- scale processing, though recital 91 provides some guidance.[14]
第37條第1項第b款及c款規定，要觸發DPO之指派，個資運用需達到大規模程度。雖然前言第91點提供了一些指導[14]，但GDPR對何謂大規模運用並無定義。

Indeed, it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop for identifying in more specific and/or quantitative terms what constitutes '*large scale*' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.
的確，要訂出一個精確的運用資料數量或涉及人數之數字，且於所有情形皆可適用，是不可能的。但即使如此，也不能排除在經過一段時間後，對於某些常見的運用業務怎樣構成「*大規模*」，可發展出以較具體且/或量化的條件判斷之標準實務做法。WP29亦規劃藉由分享、公開指派DPO之相關門檻示例，以就此一發展作出貢獻。

In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
無論如何，WP29建議於判斷運用作業是否屬大規模作業時，應特別考量以下因素：

- The number of data subjects concerned - either as a specific number or as a proportion

[14] According to the recital, '*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*' would be included, in particular. On the other hand, the recital specifically provides that '*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*'. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus processing of data of a whole country or across Europe); there is a large grey zone in between these extremes. In addition, it should be borne in mind that this recital refers to data protection impact assessments. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.
依據前言，特別是「*於區域、國家或超國家層級運用大量個資為目的並可能影響大量當事人且可能造成高度風險之大規模運用作業*」將包括在內。另一方面，該前言也明確指出「*若由個別醫師、其他專業醫療保健人員或律師運用關於其病患或客戶之個資，則不應視為大規模運用個資*」。在此應留意，前言雖就運用作業之規模提供極端之範例（個別醫師辦理之運用作業，相對於全國或全歐洲之資料運用），在這些極端之間仍有相當大之灰色地帶。此外，亦應留意此前言係闡述個資保護影響評估事宜，意味部分要件可能僅適用該相關事項，而於指派DPO時並非必然同等適用。

of the relevant population
涉及之當事人數—是否達到一定數量或占相關人口之一定比例

- The volume of data and/or the range of different data items being processed
  運用之資料量及/或不同資料項目範圍
- The duration, or permanence, of the data processing activity
  資料運用作業之期間或持續性
- The geographical extent of the processing activity
  運用作業之地理涵蓋範圍

Examples of large-scale processing include:
大規模運用的例子包括：

- processing of patient data in the regular course of business by a hospital
  醫院一般作業對病患資料之運用
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
  運用個人使用城市大眾運輸系統之旅行資料（例如以票卡資料追蹤）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
  國際速食連鎖企業為統計目的，由專業之受託運用者對顧客即時地理位置資料之運用
- processing of customer data in the regular course of business by an insurance company or a bank
  保險公司或銀行一般作業上對客戶資料之運用
- processing of personal data for behavioural advertising by a search engine
  搜尋引擎為投放行為(定向)廣告對個人資料之運用
- processing of data (content, traffic, location) by telephone or internet service providers
  電信或網路服務提供者對資料（內容、流量、位置）之運用

Examples that do not constitute large-scale processing include:
不會構成大規模資料運用的例子包括：

- processing of patient data by an individual physician
  個別醫師對病患資料之運用

- processing of personal data relating to criminal convictions and offences by an individual lawyer
  個別律師對刑事前科及犯罪相關之個人資料運用

2.1.4 'REGULAR AND SYSTEMATIC MONITORING'
經常性且系統性之監控

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but the concept of '*monitoring of the behaviour of data subjects*' is mentioned in recital 24[15] and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.
經常性且系統性監控當事人之概念於GDPR中並無定義，但前言第24點已提及「*監控當事人行為*」之概念[15]，且明確包括網路上所有形式之追蹤與剖析，及為投放行為(定向)廣告之目的之行為。

However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.[16]
然而，監控之概念並不限於網路環境，線上追蹤僅應視為監控當事人行為的其中一例[16]。

WP29 interprets 'regular' as meaning one or more of the following:
WP29就「經常性」之解釋，係指以下之一項或多項情形：

- Ongoing or occurring at particular intervals for a particular period
  具持續性或於特定期間內特定間隔發生
- Recurring or repeated at fixed times
  於固定時間反覆或重複發生

---

[15] *'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'.*
「*為決定該資料運用是否可受認定為監控該當事人之行為，應確認該當事人是否於網路上被追蹤，包含以個人資料運用技術對自然人進行剖析的潛在後續利用，尤其是為了作成與其有關的決策，或為分析或預測其個人偏好、行為及態度*」。

[16] Note that Recital 24 focuses on the extra-territorial application of the GDPR. In addition, there is also a difference between the wording '*monitoring of their behaviour*' (Article 3(2)(b)) and *'regular and systematic monitoring of data subjects'* (Article 37(1)(b)) which could therefore be seen as constituting a different notion.
須留意前言第24點係聚焦於GDPR之域外適用。此外，「*監控其行為*」（第3條第2項第b款）與「*對當事人經常性且系統性之監控*」文字上有所不同，故應視為不同之概念。

- Constantly or periodically taking place
  常態性或定期發生

WP29 interprets 'systematic' as meaning one or more of the following:
WP29對「系統性」之解釋，係指以下之一項或多項情形：

- Occurring according to a system
  依據一套系統設定而發生
- Pre-arranged, organised or methodical
  事先安排、有組織性或具一定方法
- Taking place as part of a general plan for data collection
  為一套整體資料蒐集計畫之一部分
- Carried out as part of a strategy
  為一項策略執行之一部分

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
可能構成對當事人經常性且系統性監控之例子包括：經營電信網路、提供電信服務、電子郵件再行銷、資料導向之行銷活動、為風險評估目的（如信用評分、保費計算、預防詐欺、洗錢偵測等）進行之剖析及評分、位置追蹤（例如以行動裝置應用程式為之）、客戶忠誠度計畫、行為(定向)廣告、透過穿戴裝置對身體狀況、體態及健康資料之監控、閉路電視、聯網裝置如智慧電表、智慧車輛、智慧家庭等。

2.1.5 SPECIAL CATEGORIES OF DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES
特種資料與刑事前科及犯罪資料

Article 37(1)(c) addresses the processing of special categories of data pursuant to Article 9, and personal data relating to criminal convictions and offences set out in in Article 10.

Although the provision uses the word 'and', there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say 'or'.
第37條第1項第c款，係規範對第9條所規定特種資料，及第10條所規定刑事前科及犯罪相關個資之運用。條文文字雖用刑事前科「及」犯罪，但並無必需同時適用該二項標準之政策理由。因此，該文字應視為刑事前科「或」犯罪。

2.2. DPO of the processor
受託運用者之DPO

Article 37 applies to both controllers[17] and processors[18] with respect to the designation of a DPO. Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).
第37條就指派DPO事宜，對控管者[17]及受託運用者[18]均適用。依哪一方符合強制指派DPO標準決定，有時僅其中一方必須指派DPO，有時兩者均應指派（如均應指派，則DPO間應相互合作）。

It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.
此處須留意，即使控管者符合強制指派DPO之標準，其受託運用者亦不必然須指派DPO，然而無論是否符合標準均指派DPO，可謂優良做法。

Examples:
範例：

- A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively

[17] The controller is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.
依據第4條第7款定義，控管者係指決定資料運用目的及方法之個人或機構。
[18] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.
依據第4條第8款定義，受託運用者係指代控管者運用資料之個人或機構。

limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

一家於單一城鎮內經營家電經銷之小型家族企業，其合作之受託運用者，係以提供網站分析服務與協助定向廣告與行銷為核心業務。此家族企業及其顧客之活動，因其顧客數量少、業務有限，不會構成「大規模」之資料運用。但該受託運用者之活動，因其有許多與此家族企業類似之客戶，其整體資料運用作業即屬大規模運用。因此該受託運用者應依第37條第1項第b款規定，指派一名DPO。同時，此家族企業則無指派DPO之義務。

- A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

  一家中型瓷磚製造商將職業健康服務外包予外部受託運用者，而該受託運用者有許多類似之客戶。因此該受託運用者應依第37條第1項第c款之大規模運用規定指派一名DPO。然而，該製造商則不必然有指派DPO之義務。

The DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

當受託運用者指派之DPO，其本身職權即屬資料控管者（如人資、資訊、物流等）時，亦應監督該受託運用者組織之活動。

2.3. Designation of a single DPO for several organisations

數個組織指派一名DPO

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects[19], the supervisory authority[20]

[19] Article 38(4): '*data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation*'.
第38條第4項：「*當事人得就依本規則運用其個資及行使其義務之所有相關事宜，與個資保護長聯繫*」。

[20] Article 39(1)(e): '*act as a 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*'.
第39條第1項第e款：「*就資料運用相關事宜（包括第36條所述之事前諮商）作為與監管機關間之聯絡點，並與其於適當時就任何其他事宜進行諮商。*」

but also internally within the organisation, considering that one of the tasks of the DPO is *'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this Regulation'*.[21]
第37條第2項允許企業集團僅指派一名DPO，只要「*各據點皆易於聯繫*」該DPO。可及性之概念係指就DPO擔任當事人[19]、監管機關[20]與組織內部之聯絡點的任務而言，其中一項是「*告知與建議控管者、受託運用者及執行運用作業之員工依據本規則應盡之義務*」[21]。

In order to ensure that the DPO, whether internal or external, is accessible it is important to make sure that their contact details are available in accordance with the requirements of the GDPR.[22]
為確保DPO可被聯繫（無論內部或外部），重點在於確認其依GDPR之要求提供詳細聯絡資訊[22]。

He or she, with the help of a team if necessary, must be in a position to efficiently communicate with data subjects[23] and cooperate[24] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.
其必須具有可有效率地與當事人溝通[23]，並與相關監管機關合作之職位[24]（必要時可由團隊協助）。此也意味著此溝通必須與監管機關及相關當事人以一種或數種語言進行。DPO之可用性（無論是與員工處於同一場所內、透過熱線電話或其他安全之通訊方式）係確保當事人可聯繫DPO之關鍵。

According to Article 37(3), a single DPO may be designated for several public authorities or

[21] Article 39(1)(a).
第39條第1項第a款。
[22] See also Section 2.6 below.
另參照第2.6節以下說明。
[23] Article 12(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.'*
第12條第1項：「*控管者應採取適當措施，以簡潔、透明、易懂且便於取得之形式，使用清晰、平易的語言文字，提供當事人第13條及第14條所述之所有資訊，並與當事人依第15條至第22條及第34條規定就關於資料運用進行所有溝通，尤其是任何明確指涉兒童之資訊。*」
[24] Article 39(1)(d) *: 'to cooperate with the supervisory authority'*
第39條第1項第d款：「*與監管機關合作*」。

bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

依據第37條第3項，數個公務機關或機構於衡量其組織架構及規模後，可指派單一DPO。前述有關資源及溝通之考量在此亦適用。因DPO掌理許多不同之任務，控管者或受託運用者必須確保此單一DPO即使為數個公務機關或機構所指派，仍可有效率地執行任務（必要時可由團隊協助）。

2.4. Accessibility and localisation of the DPO
DPO之可及性及在地化

According to Section 4 of the GDPR, the accessibility of the DPO should be effective.

依據GDPR第4節規定，DPO應具備有效之可及性。

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union.

為確保DPO之可及性，WP29建議，無論控管者或受託運用者是否於歐盟境內設立，DPO均應設置於歐盟境內。

However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union[25], a DPO may be able to carry out his or her activities more effectively if located outside the EU.

然而，不排除於某些情形下，控管者或受託運用者於歐盟境內未設置據點時[25]，DPO如設於歐盟境外，可能可更有效執行其業務。

2.5. Expertise and skills of the DPO
DPO之專業及技能

Article 37(5) provides that the DPO '*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*'. Recital 97 provides that the necessary level of expert

[25] See Article 3 of the GDPR on the territorial scope.
詳參GDPR第3條關於領域範圍之規定。

knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.
第37條第5項規定DPO「*應以其專業能力，尤以其對資料保護法規與實務之專業知識，及確實達成第39條所述任務之能力，為指派基礎*」。前言第97點則敘明，必要之專業知識程度應視所執行之資料運用作業，及所運用之個人資料所需之保護措施而定。

- Level of expertise
  專業程度

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.
對專業程度之要求並無嚴格定義，但必須與組織所運用資料之敏感性、複雜度及資料量相應。舉例而言，當資料運用作業特別複雜，或涉及大量敏感資料時，DPO可能需要更高之專業程度及支援。該組織係系統性將個資傳輸至歐盟境外或偶爾為之，對DPO專業程度之要求亦有所不同。因此，DPO之選任應依組織內產生之資料保護相關問題適當考量並謹慎為之。

- Professional qualities
  專業能力

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs must have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.
儘管第37條第5項並未明確規定指派DPO時應考量之專業能力，但相關要件是DPO必須具備國內及歐盟資料保護法規與實務專業，及對GDPR之深入了解。監管機關如可推動適當的、定期的DPO訓練，亦有所幫助。

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

對產業及控管者之組織的知識是有助益的。DPO亦應對控管者之資料運用作業、資訊系統、資料安全及資料保護需求有深入了解。

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.
如係公務機關或機構，DPO則亦應對該組織之行政規章及程序有充分的知識。

- Ability to fulfil its tasks
  達成任務之能力

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing[26], data subjects' rights[27], data protection by design and by default[28], records of processing activities[29], security of processing[30], and notification and communication of data breaches.[31]
DPO達成其所肩負任務之能力，應解釋為同時包含其個人素質、知識，及其於組織內之職位。個人素質，應包括如誠信及高度之職業倫理；DPO之首要考量應係促成GDPR之法遵。DPO於培養組織內資料保護文化扮演關鍵角色，且有助於GDPR中重要元素如資料運用原則[26]、當事人權利[27]、以資料保護為系統設計目的及預設選項[28]、運用作業紀錄[29]、運用作業安全[30]，及資料侵害通報及溝通[31]等之執行。

- DPO on the basis of a service contract
  以服務契約為基礎之DPO

The function of the DPO can also be exercised on the basis of a service contract concluded

[26] Chapter II.
第二章。
[27] Chapter III.
第三章。
[28] Article 25.
第25條。
[29] Article 30.
第30條。
[30] Article 32.
第32條。
[31] Articles 33 and 34.
第33及第34條。

with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that each member of the organisation exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.
DPO之功能亦可由控管者/受託運用者與組織以外之個人或組織簽署服務契約來執行。如係後者（與組織簽署契約）之情形，則重要的是此簽約對象之組織中執行DPO功能之成員均符合GDPR第4節規定中所有應適用之要求（例如成員中無人有利益衝突）。同樣重要的是，每一位此種成員皆受GDPR條文之保護（例如不因執行DPO業務而遭不當終止服務契約，及組織中執行DPO業務之個人不因此而遭不當解僱等）。同時，亦可以團隊方式結合數人之技能及特長，得以更有效率地服務其客戶。

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.
為求法律上之明確性及良好之組織，並防止團隊成員之利益衝突，建議DPO團隊內應有明確分工，並就每個客戶指派一人為主要聯絡人及「負責」人。在服務契約中敘明前述各事項乃常見且實用。

2.6. Publication and communication of the DPO's contact details
DPO詳細聯絡資訊之公布及傳達

Article 37(7) of the GDPR requires the controller or the processor:
GDPR第37條第7項要求控管者或受託運用者應：

- to publish the contact details of the DPO and
  公布DPO之詳細聯絡資訊，並
- to communicate the contact details of the DPO to the relevant supervisory authorities.
  將DPO之詳細聯絡資訊提供予相關監管機關。

The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) and the supervisory authorities can easily and directly contact the DPO

without having to contact another part of the organisation. Confidentiality is equally important: for example, employees may be reluctant to complain to the DPO if the confidentiality of their communications is not guaranteed.
此要求之目的係為確保（無論組織內外之）當事人及監管機關可以容易地、直接地與DPO聯繫，而無需聯繫組織之其他部門。保密亦具同等重要性，舉例而言，如員工與DPO間之通訊保密未受保障，則其可能不願向DPO提出申訴。

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)).
依據歐盟及會員國法律，DPO就其任務之執行情形應予保密（第38條第5項）。

The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and/or a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.
DPO之詳細聯絡資訊，應包含可使當事人及監管機關容易與DPO取得聯繫之資訊（郵寄地址、專線電話及/或專用電郵信箱）。為與大眾溝通，於適當情況，亦可提供其他通訊方式，例如專用熱線電話或於組織網站上與DPO聯繫之專用連絡表單。

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do so, it is for the controller or the processor and the DPO to decide whether this is necessary or helpful in the particular circumstances.[32]
第37條第7項並非要求所公布之聯絡資訊應包含DPO之姓名。雖然公布姓名或為優良作法，但在特定情形下公布DPO姓名是否必要或有助益，應由控管者或受託運用者與DPO決定[32]。

However, communication of the name of the DPO to the supervisory authority is essential in order for the DPO to serve as contact point between the organisation and the supervisory authority (Article 39(1)(e).
然而，將DPO之姓名提供予監管機關，係DPO作為組織與監管機關間聯絡點之重要事

[32] It is notable that Article 33(3)(b), which describes information that must be provided to the supervisory authority and to the data subjects in case of a personal data breach, unlike Article 37(7), specifically also requires the name (and not only the contact details) of the DPO to be communicated.
應留意第33條第3項第b款闡述了如發生個資外洩事件時必須提供予監管機關及當事人之資訊，且與第37條第7項規定不同的是，該款明確要求提供DPO之姓名（而非僅聯絡資訊）。

項（第39條第1項第e款）。

As a matter of good practice, the WP29 also recommends that an organisation informs its employees of the name and contact details of the DPO. For example, the name and contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.
WP29亦建議，組織將其DPO之姓名及聯絡資訊告知員工，係為優良做法。舉例而言，DPO之姓名及聯絡資訊可由組織內網、內部電話表及組織圖等方式對內公布。

3 Position of the DPO
DPO之職位

3.1. Involvement of the DPO in all issues relating to the protection of personal data
DPO對所有個資保護相關事宜之參與

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is *'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'*.
GDPR第38條規定，控管者及受託運用者應確保DPO「*適切且即時地參與所有個資保護相關事宜*」。

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.[33] Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.
DPO或其團隊儘量於所有資料保護相關事宜之前期即參與其中，具關鍵重要性。就個資保護影響評估而言，GDPR對DPO於前期之參與已有明文規定，並明確指出控管者辦理該影響評估時，應尋求DPO之建議[33]。確保DPO於一開始即知情且受到諮詢，將可促進對GDPR之法遵、推動以隱私保護為系統設計目的之方法，故應係組織內部治理之標

[33] Article 35(2).
第35條第2項。

準程序。此外，組織內部將DPO視為可共同討論之夥伴，並將其納入組織內資料運用作業相關之工作小組，亦至關重要。

Consequently, the organisation should ensure, for example, that:
因此，舉例而言，組織應確保以下事項：

- The DPO is invited to participate regularly in meetings of senior and middle management.
  DPO應受邀定期參與管理高層及中階主管之會議。
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
  進行之決策可能對資料保護產生影響時，建議DPO應在場。所有相關資訊均應即時傳遞予DPO，以利其提供充足之建議。
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
  DPO之意見必須予適當尊重。如出現意見不同情形，WP29建議記錄未遵循DPO建議之理由，為優良做法。
- The DPO must be promptly consulted once a data breach or another incident has occurred.
  如發生資料侵害或其他事故，應即時諮詢DPO。

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.
控管者或受託運用者可於適當時機研擬資料保護指引或計畫，規範何時應諮詢DPO。

3.2. Necessary resources
必要資源

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'*. The following items, in particular, are to be considered:
GDPR第38條第2項要求組織應以「*提供執行〔其〕任務、存取個資及個資運用作業，*

及維持其專業知識之必要資源」支援DPO。特別應考量以下項目：

- Active support of the DPO's function by senior management (such as at board level).
  於管理高層（如董事會層級）積極支持DPO之功能。
- Sufficient time for DPOs to fulfil their duties. This is particularly important where an internal DPO is appointed on a part-time basis or where the external DPO carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
  給予DPO充足時間完成職責。尤其是如果DPO係由組織內部人員兼任，或外部DPO於執行資料保護業務外亦具其他職責時，特別重要。否則，各項工作優先順序之衝突可能造成DPO之職責遭到忽略。有充足時間來執行DPO之任務至關重要。如DPO係兼任，則明定一定比例之時間執行DPO工作係優良做法。決定執行相關功能所需之時間及DPO職責適當之優先層級，以及由DPO（或由組織）研擬工作計畫，亦係優良做法。
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
  適當之財務資源、基礎設施（場所、設備、器材）及人員之充足支援。
- Official communication of the designation of the DPO to all staff to ensure that their existence and function are known within the organisation.
  就DPO之指派正式傳達所有員工，以確保組織內部知悉其存在及功能。
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
  DPO應可取得其他必需之服務，如人資、法務、資訊、資安等，使其可自該等服務管道獲得必要之支援、資源投入及資訊。
- Continuous training. DPOs must be given the opportunity to stay up to date with regard to developments within the field of data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional

development, such as participation in privacy fora, workshops, etc.
持續之訓練。DPO必須有機會持續瞭解資料保護領域之新發展。訓練之目標應係持續增進DPO之專業程度，且應鼓勵DPO參與資料保護相關訓練課程及其他形式之專業發展，如隱私論壇、工作坊等。

- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.
視組織大小及結構，設置DPO團隊（即DPO本人及其成員）或有其必要。在此情形下，團隊內部之架構及其成員之任務及職責應明確訂定。同理，當DPO之功能係由外部服務提供者執行時，若干個人組成之團隊可指派一名對客戶的主要聯絡人，有效地以團隊方式實際執行DPO之任務。

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.
一般而言，運用作業越複雜及/或敏感，必須給予DPO之資源就越多。資料保護之功能須有效，且具備與所辦理之資料運用作業相對應之充分資源。

3.3. Instructions and '*performing their duties and tasks in an independent manner*'
指示及「*獨立執行其職責及任務*」

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO '*does not receive any instructions regarding the exercise of [his or her] tasks.*' Recital 97 adds that DPOs, '*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*'.
第38條第3項確立了若干確保DPO可於組織中執行任務時具充足自主性之基本保障事項。特別是要求控管者/受託運用者應確保DPO「*免於接受任何有關執行（其）任務之指示*」。前言第97點亦補充說明DPO「*無論是否受僱於控管者，都應該能以獨立方式執行其職責和任務*」。

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.

此意味DPO於執行第39條規定之任務時，DPO不得接受應如何處理事務之指示，例如應達成何種結果、如何調查申訴案或是否應諮詢監管機關等。此外，DPO不得就資料保護法規相關議題，接受應採特定見解之指示，例如採特定之法規解釋等。

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

然而，DPO之自主性，不代表其具有超越第39條所規定任務範圍以外之決策權。

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.[34] If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO '*shall directly report to the highest management level of the controller or the processor'*. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.

控管者或受託運用者仍肩負遵守資料保護法規之責，且應能證明其合規[34]。如控管者或受託運用者之決策與GDPR及DPO之建議不符，應賦予DPO向最高管理階層，及此決策之決策者，釐清其不同意見之可能性。就此部分，第38條第3項規定，DPO「*應直接向控管者或受託運用者之最高管理階層報告*」。此直接報告可確保高層管理者（例如董事會）知悉DPO依其告知及向控管者或受託運用者提供建議之職務，所提出之意見及建議事項。另一種直接報告之範例為撰擬DPO業務年度報告，提交予最高管理階層。

3.4. Dismissal or penalty for performing DPO tasks

DPO因執行任務而遭解僱或處罰

Article 38(3) requires that DPOs should *'not be dismissed or penalised by the controller or*

[34] Article 5(2).
第5條第2項。

the processor for performing [their] tasks'.
第38條第3項規定DPO「*不應因執行〔其〕任務而遭控管者或受託運用者解僱或處罰*」。

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.
此要求強化了DPO之自主性，且有助於確保DPO獨立作業，並就執行其資料保護業務享有充足之保護。

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.
因執行其DPO之職責而導致其受處罰，僅於GDPR中受禁止。例如，DPO可能認為某項特殊的運用可能導致高風險，而建議控管者或受託運用者進行個資保護影響評估，但控管者或受託運用者並不同意DPO之評估。在此情形下，DPO不應因提出此項建議而遭解僱。

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.
處罰可能採取不同之形式，也可能是直接或間接的。可能包括例如不予升職或延遲升職、阻擋職涯發展、不提供其他員工可得之福利等。不必然需實際處罰，只要處罰DPO是與其業務有關，僅是威脅即足以構成。

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).
DPO仍可因執行其任務以外之正當理由（例如竊盜、生理、心理、性騷擾或其他類似之嚴重不當行為等）被解僱，此係一般之管理原則，與適用國內契約或勞工、刑事法律之其他員工或契約人員相同。

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

在此應留意，GDPR並未明定如何與何時可解僱或以他人取代DPO。然而，DPO之合約越穩定，不受不當解僱之保障越高，其將越有可能獨立執行職務。因此，WP29樂見各組織朝此方向努力。

3.5. Conflict of interests

利益衝突

Article 38(6) allows DPOs to '*fulfil other tasks and duties*'. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests*'.

第38條第6項容許DPO「*執行其他任務及職責*」。但該項亦要求該組織確保「*此任務或職責不會造成利益衝突*」。

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

無利益衝突之概念與獨立執行職務密切相關。雖允許DPO可有其他功能，但僅在不造成利益衝突之前提下，方可賦予DPO其他任務及職責。確切來說，此意味DPO不得擔任組織中決定個資運用目的及方式之職位。因各組織之組織結構不同，此部分必須依個案考量。

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

一般而言，組織內利益衝突之職位可能包含管理高層（如執行長、營運長、財務長、醫療長、行銷部主管、人資部主管、技術長等），但如組織結構中較低階之職位會決定個資運用之目的及方式，則亦可能包含該職位。此外，例如外部DPO代表控管者或受託運用者就資料保護爭議至法院出庭時，亦可能發生利益衝突。

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:
依個別組織之業務、規模及結構不同，以下可為控管者或受託運用者之優良做法：

- to identify the positions which would be incompatible with the function of DPO
  確認與DPO功能無法相容之職位
- to draw up internal rules to this effect in order to avoid conflicts of interests
  就此擬定避免利益衝突之內規
- to include a more general explanation about conflicts of interests
  包含對利益衝突之一般性解釋文字
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
  聲明其DPO就其擔任DPO之功能並無利益衝突，以提高對此要求之意識
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally
  將相關安全機制納入組織內規，並確保DPO之職缺公告或服務契約足夠精確與詳盡，以避免利益衝突。此處亦應留意利益衝突可能依DPO係內部或外部雇用人員，而有不同之形式。

4 Tasks of the DPO
DPO之任務

4.1. Monitoring compliance with the GDPR
監督對GDPR之法遵事宜

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO '*should assist the controller or the processor*

to monitor internal compliance with this Regulation'.
第39條第1項第b款賦予DPO任務之一係監督對GDPR之法遵事宜。前言第97點進一步說明DPO「*應協助控管者或受託運用者監督組織內部對本規則之遵循事宜*」。

As part of these duties to monitor compliance, DPOs may, in particular:
具體而言，DPO得於監督法遵之職責範圍內：

- collect information to identify processing activities
  蒐集資訊以確認運用作業
- analyse and check the compliance of processing activities
  分析並檢視運用作業之法遵
- inform, advise and issue recommendations to the controller or the processor
  通知、勸告及提出建議予控管者或受託運用者

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.
監督法遵並不表示發生未遵法事件時，應由DPO本人負責。GDPR明確規定，應「*採取適當的技術性和組織性措施，確保並得以證明依本規則執行運用*」者，為控管者而非DPO（第24條第1項）。資料保護法遵是資料控管者之公司責任，而非DPO之責任。

4.2. Role of the DPO in a data protection impact assessment
DPO於個資保護影響評估中之角色

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice'* of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35*'.
依據第35條第1項規定，於必要時辦理個資保護影響評估（DPIA）係控管者而非DPO之任務。然而，DPO於協助控管者上，可扮演非常重要且實用之角色。第35條第2項依

循以資料保護為系統設計目的之原則，明確要求控管者於辦理DPIA時「*應徵詢DPO之意見*」。而第39條第1項第c款，則賦予DPO「*應依第35條規定就〔DPIA〕提供建議並監督其執行*」之職責。

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others [35]:
WP29建議控管者應至少就以下事宜徵詢DPO之建議[35]：

- whether or not to carry out a DPIA
  是否辦理DPIA
- what methodology to follow when carrying out a DPIA
  辦理DPIA時應採取之方法
- whether to carry out the DPIA in-house or whether to outsource it
  DPIA應由組織內部辦理或委外辦理
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
  應採取何種安全措施（包含技術性及組織性措施）以降低當事人權利及利益之風險
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR
  個資保護影響評估是否依正確方式辦理，及其結論（是否於運用前辦理及採取何種安全措施）是否遵循GDPR規範

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account[36].

---

[35] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have '*at least*' the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail.
第39條第1項提及DPO之任務，並敘明DPO「*至少*」應有以下任務。因此，並未禁止控管者分派第39條第1項明文規定範圍以外之其他任務予DPO或將這些任務作更明確、詳細之說明。

[36] Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure* ***and to be able to demonstrate*** *that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'.
第24條第1項規定「*考量運用之性質、範圍、背景和目的，以及不同可能性與嚴重性對自然人的權利及自由造成之風險，控管者應採取適當的技術性和組織性措施，確保****並得以證明****依本規則執行運用。必要時應檢視並*

如控管者不同意DPO之諮詢意見，DPIA文件中應以書面明確記載未採納該意見之正當理由[36]。

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.
WP29進一步建議控管者，於DPO之合約及提供予員工、管理階層（及其他有關之利害關係人）之資訊等，明確指出DPO之確切任務及涵蓋範圍，特別是辦理DPIA之相關事項。

4.3. Cooperating with the supervisory authority and acting as a contact point
與監管機關合作並作為聯絡點

According to Article 39(1)(d) and (e), the DPO should '*cooperate with the supervisory authority*' and '*act as a 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'*.
依據第39條第1項第d款及e款，DPO應「*與監管機關合作*」並「*就資料運用相關事宜，包含第36條規定之事前諮詢，作為對監管機關之聯絡點，並於適當時就任何其他事宜向監管機關諮詢*」。

These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.
這些任務涉及本指引導言中提及DPO作為「促進者」之角色。DPO係以作為聯絡點方式使監管機關便於取得文件及資訊，以執行第57條所述之任務，並行使第58條所述之

更新這些措施」。

調查、糾正、授權、建議等權力。如前所述，DPO就其任務執行事宜，依據歐盟或會員國法規負有保密之責（第38條第5項）。然而，此保密義務並非禁止DPO聯繫監管機關並徵詢其意見。第39條第1項第e款規定，DPO亦可於適當時就任何其他事宜徵詢監管機關之意見。

4.4. Risk-based approach

以風險為基礎之方法

Article 39(2) requires that the DPO '*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*'.

第39條第2項要求DPO「*基於運用之性質、範圍、脈絡及目的，考量運用作業的相關風險*」。

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

此條文重述了一項與DPO日常業務許多方面皆相關之一般常識性原則。本質上，此條文要求DPO應將業務排列優先順序，努力聚焦在資料保護風險較高之議題。此非謂DPO即應忽略對風險相對較低資料運用作業之法遵監督，而係表示其主要應專注於風險較高之領域。

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

此種有選擇性的且務實的方法，應可幫助DPO就辦理DPIA應採取之方式、何種範圍應辦理內部或外部資料保護稽核、應提供予負責資料運用作業員工或管理階層何種內部訓練，及應投入其較多時間及資源於何種運用作業等事宜，向控管者提供諮詢意見。

4.5. Role of the DPO in record-keeping

DPO於紀錄保存之角色

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to '*maintain a record of processing operations under its responsibility*' or *'maintain a record of all categories of processing activities carried out on behalf of a controller'*.
依第30條第1項及第2項規定，應「*維護其所負責之運用作業紀錄*」或「*維護其代控管者辦理之所有運用作業類別紀錄*」者，係控管者或受託運用者，而非DPO。

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[37]
實務上，DPO常會依據組織內負責運用個資部門提供之資訊，建立、保留一份運用作業及登記清冊。此作法於許多現行國內法及歐盟機關、機構所適用之資料保護規章中，已訂有明文[37]。

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or the processor. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
第39條第1項所列之工作項目，乃對DPO之最低限度要求。因此，控管者或受託運用者就其所負責之運用作業，指派DPO維護紀錄，亦無不可。該等紀錄應視為DPO執行其監督法遵事宜，及向控管者或受託運用者提供資訊及建議等任務之工具之一。

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.
無論如何，依第30條規定應保留之紀錄，亦應視為使控管者及監管機關，得應要求檢視組織所辦理所有個資運用作業之工具。因此，該紀錄係法遵之先決條件，與有效之課責性措施。

[37] Article 24(1)(d), Regulation (EC) 45/2001.
歐盟第45/2001號規則第24條第1項第d款。

5 ANNEX - DPO GUIDELINES: WHAT YOU NEED TO KNOW
附錄—DPO指引：你應該要知道的事

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the General Data Protection Regulation (GDPR) to appoint a DPO.
此附錄之目的，係以簡化、易讀之形式，解答各組織依據一般資料保護規則（GDPR）所定之新要件指派DPO事宜之重要問題。

Designation of the DPO
DPO之指派

1 Which organisations must appoint a DPO?
什麼組織必須指派DPO？

The designation of a DPO is an obligation:
於下列情形下，有義務指派DPO：

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
  運用作業係由公務機關或機構辦理（無論運用之資料為何）
- if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
  控管者或受託運用者之核心業務包含對當事人進行經常性、系統性大規模監控之運用作業
- if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences
  控管者或受託運用者之核心業務，包含大規模運用特種資料或與刑事前科及犯罪相關之個人資料

Note that Union or Member State law may require the designation of DPOs in other situations as well. Finally, even if the designation of a DPO is not mandatory, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts. When an organisation

designates a DPO on a voluntary basis, the same requirements will apply to his or her designation, position and tasks as if the designation had been mandatory.
此處須留意，歐盟或會員國法規可能要求於其他情形下亦須指派DPO。最後，即使於非強制指派DPO之情形下，組織有時會發現自願性指派DPO有其益處。第29條個資保護工作小組（WP29）亦鼓勵此自願性之努力。如組織自願指派DPO，該DPO之指派、職位及任務即適用強制指派之標準。

Source: Article 37(1) of the GDPR
資料來源：GDPR第37條第1項

2 What does 'core activities' mean?
何謂「核心業務」？

'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.
「核心業務」可視為達成控管者或受託運用者目標之關鍵性作業。此亦包含控管者或受託運用者以運用資料為其不可分割的一部分之所有業務。例如，運用病人病歷等醫療資料應視為任何一所醫院之核心業務之一，故醫院亦必須指派DPO。

On the other hand, all organisations carry out certain supporting activities, for example, paying their employees or having standard IT support activities. These are examples of necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.
另一方面，某些支援性業務是所有組織均會辦理的，如支付員工薪資，或進行一般性之資訊科技支援工作。此係組織之核心業務或主要經營領域所必須具備之支援功能。即使該業務是必要的或不可缺的，一般仍視為附屬功能而非核心業務。

Source: Article 37(1)(b) and (c) of the GDPR
資料來源：GDPR第37條第1項第b款及c款

3 What does 'large scale' mean?
何謂「大規模」？

The GDPR does not define what constitutes large-scale processing. The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
GDPR對何謂大規模運用並無定義。WP29建議於判斷運用作業是否屬大規模時，應特別考量以下因素：

- the number of data subjects concerned - either as a specific number or as a proportion of the relevant population
  涉及之當事人數—是否達到一定數量或占相關人口之一定比例
- the volume of data and/or the range of different data items being processed
  運用之資料量及/或不同資料項目範圍
- the duration, or permanence, of the data processing activity
  資料運用作業之期間或持續性
- the geographical extent of the processing activity
  運用作業之地理涵蓋範圍

Examples of large scale processing include:
大規模運用的例子包括：

- processing of patient data in the regular course of business by a hospital
  醫院一般作業對病患資料之運用
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
  運用個人使用城市大眾運輸系統之旅行資料（例如以票卡資料追蹤）
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
  國際速食連鎖企業為統計目的，由專業之受託運用者對顧客即時地理位置資料之運用
- processing of customer data in the regular course of business by an insurance company or a bank
  保險公司或銀行一般作業上對客戶資料之運用
- processing of personal data for behavioural advertising by a search engine
  搜尋引擎為投放行為(定向)廣告對個人資料之運用

- processing of data (content, traffic, location) by telephone or internet service providers
  電信或網路服務提供者對資料（內容、流量、位置）之運用

Examples that do not constitute large-scale processing include:
不會構成大規模資料運用的例子包括：

- processing of patient data by an individual physician
  個別醫師對病患資料之運用
- processing of personal data relating to criminal convictions and offences by an individual lawyer
  個別律師對刑事前科及犯罪相關之個人資料運用

Source: Article 37(1)(b) and (c) of the GDPR
資料來源：GDPR第37條第1項第b款及c款

4 What does 'regular and systematic monitoring' mean?
何謂「經常性且系統性監控」？

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.
經常性且系統性監控當事人之概念於GDPR中並無定義，但明顯包含所有形式，包括為投放行為定向廣告所做的網路追蹤與剖析。然而，監控之概念並不限於網路環境。

Examples of activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.
可能構成對當事人經常性且系統性監控之例子包括：經營電信網路、提供電信服務、電子郵件再行銷、資料導向之行銷活動、為風險評估目的（如信用評分、保費計算、預防詐欺、洗錢偵測等）進行之剖析及評分、位置追蹤（例如以行動裝置應用程式為

之）、客戶忠誠度計畫、行為（定向）廣告、透過穿戴裝置對身體狀況、體態及健康資料之監控、閉路電視、聯網裝置如智慧電表、智慧車輛、智慧家庭等。

WP29 interprets 'regular' as meaning one or more of the following:
WP29就「經常性」之解釋，係指以下之一項或多項情形：

- ongoing or occurring at particular intervals for a particular period
  具持續性或於特定期間內特定間隔發生
- recurring or repeated at fixed times
  於固定時間反覆或重複發生
- constantly or periodically taking place
  常態性或定期發生

WP29 interprets 'systematic' as meaning one or more of the following:
WP29對「系統性」之解釋，係指以下之一項或多項情形：

- occurring according to a system
  依據一套系統設定而發生
- pre-arranged, organised or methodical
  事先安排、有組織性或具一定方法
- taking place as part of a general plan for data collection
  為一套整體資料蒐集計畫之一部分
- carried out as part of a strategy
  為一項策略執行之一部分

Source: Article 37(1)(b) of the GDPR
資料來源：GDPR第37條第1項第b款

5 Can organisations appoint a DPO jointly? If so, under what conditions?
多個組織可否共同指派一名DPO？若可，條件為何？

Yes. A group of undertakings may designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation. In order to ensure that the DPO is accessible, whether internal or external, it is important to make sure that their contact details are available. The DPO, with

the help of a team if necessary, must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

可以。企業集團可指派單一DPO，只要此DPO能「*便於各據點聯繫*」。可及性之概念係指DPO擔任當事人、監管機關及組織內部聯絡點之任務。為確保DPO之可及性（無論內部或外部），重要的是應確認DPO之聯絡資訊為正確可用的。其必須具有可有效率地與當事人溝通，並與相關監管機關合作之職位（必要時可由團隊協助）。此也意味著該溝通必須與監管機關及相關當事人以一種或數種語言進行。DPO之可用性（無論是與員工處於同一場所內、透過熱線電話或其他安全之通訊方式聯繫）係確保當事人可聯繫DPO之關鍵。

A single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is in charge of a variety of tasks, the controller or the processor must ensure that a single DPO, with the help of a team if necessary, can perform these efficiently despite being designated for several public authorities and bodies.

多個公務機關或機構於衡量其組織架構及規模後，可指派單一DPO。前述有關資源及溝通之考量在此亦適用。因DPO掌理許多不同之任務，控管者或受託運用者必須確保此單一DPO即使被多個公家機關或機構指派，仍可有效率地執行此任務（必要時可由團隊協助）。

Source: Article 37(2) and (3) of the GDPR

資料來源：GDPR第37條第2項及第3項

6 Where should the DPO be located?
DPO應設置於何處？

To ensure that the DPO is accessible, the WP29 recommends that the DPO be located within the European Union, whether or not the controller or the processor is established in the European Union. However, it cannot be excluded that, in some situations where the controller or the processor has no establishment within the European Union, a DPO may be able to carry out his or her activities more effectively if located outside the EU.

為確保DPO之可及性，WP29建議，無論控管者或受託運用者是否於歐盟境內設立，

DPO均應設置於歐盟境內。然而，不排除於某些情形下，控管者或受託運用者於歐盟境內未設置據點時，DPO如設於歐盟境外，可能可更有效執行其業務。

7 Is it possible to appoint an external DPO?
是否可指派組織外部之DPO？

Yes. The DPO may be a staff member of the controller or the processor (internal DPO) or fulfil the tasks on the basis of a service contract. This means that the DPO can be external, and in this case, his/her function can be exercised based on a service contract concluded with an individual or an organisation.
可以。DPO可以是控管者或受託運用者之員工（內部DPO）或依服務契約履行任務。此表示DPO可由外部人員擔任，於此情形下，得基於與個人或組織簽訂之服務契約實踐其功能。

When the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all applicable requirements of the GDPR.
當DPO之功能係由外部服務提供者執行時，於指定之主要聯絡與「負責」該客戶之人主責下，受僱於該服務提供者的一組人，得以團隊方式有效執行DPO之任務。在此情形下，此執行DPO之外部組織中每一成員均應符合GDPR對DPO適用之所有資格要求。

For the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, the Guidelines recommend to have, in the service contract, a clear allocation of tasks within the external DPO team and to assign a single individual as a lead contact and person 'in charge' of the client.
為求法律上之明確性及良好之組織，並防止團隊成員之利益衝突，此指引建議在服務契約中敘明外部DPO團隊之分工，並指派一人為主要聯絡人及「負責」人。

Source: Article 37(6) of the GDPR
資料來源：GDPR第37條第6項

8 What are the professional qualities that the DPO should have?
DPO應具備何專業？

The DPO 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 his or her tasks.
DPO應以其專業能力，特別是對資料保護法規與實務之專業知識，及達成任務之能力，為指派之基礎。

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.
必要之專業知識程度應視所執行之資料運用作業，及所運用之資料所需之保護措施而定。舉例而言，當資料運用作業特別複雜，或涉及大量敏感資料時，DPO可能需要更高之專業程度及支援。

Relevant skills and expertise include:
相關之技能及專業包括：

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
  對國內及歐洲資料保護法規及實務之專業，包括對GDPR之深入了解
- understanding of the processing operations carried out
  對組織所辦理之資料運用作業之瞭解
- understanding of information technologies and data security
  對資訊科技及資料安全之瞭解
- knowledge of the business sector and the organization
  對產業及組織之知識
- ability to promote a data protection culture within the organization
  於組織內推動資料保護文化之能力

Source: Article 37(5) of the GDPR
資料來源：GDPR第37條第5項。

Position of the DPO DPO之職位

9 What resources should be provided to the DPO by the controller or the processor? 控管者或受託運用者應提供DPO什麼資源？

The DPO must have the resources necessary to be able to carry out his or her tasks.
DPO必須擁有使其可執行任務之必要資源。

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:
視運用作業之性質及組織業務與規模之不同，以下資源應提供予DPO：

- active support of the DPO's function by senior management
  管理高層對DPO功能之積極支持
- sufficient time for DPOs to fulfil their tasks
  讓DPO完成其任務之充足時間
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
  於適當情形下，提供充足之財務資源、基礎設施（場所、設備、器材）及人員支援
- official communication of the designation of the DPO to all staff
  就DPO之指派正式傳達予所有員工
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
  DPO應可自組織內取得其他服務，使其可從這些服務得到必要之支援、資源投入及資訊
- continuous training
  持續之訓練

Source: Article 38(2) of the GDPR
資料來源：GDPR第38條第2項

10 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner? What does 'conflict of interests' mean?
使DPO可獨立執行其任務之安全措施為何？何謂「利益衝突」？

Several safeguards exist in order to enable the DPO to act in an independent manner:
確保DPO獨立作業之安全措施如下：

- no instructions by the controllers or the processors regarding the exercise of the DPO's

tasks
控管者或受託運用者不就DPO執行任務下達任何指示

- no dismissal or penalty by the controller for the performance of the DPO's tasks
  DPO不會因執行其任務而遭控管者解僱或處罰
- no conflict of interest with possible other tasks and duties
  不會與其他可能之任務或職責產生利益衝突

The other tasks and duties of a DPO must not result in a conflict of interests. This means, first, that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.
DPO之其他任務或職責不得造成利益衝突。此意味首先DPO不得擔任組織中可決定個資運用作業目的及方式之職位。因各組織之組織結構不同，此部分必須依個案考量。

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.
一般而言，組織內利益衝突之職位可能包含管理高層（如執行長、營運長、財務長、醫療長、行銷部主管、人資部主管、技術長等），但如組織結構中較低階之職位會決定個資運用之目的及方式，則亦可能包含該職位。此外，例如外部DPO代表控管者或受託運用者就資料保護爭議至法院出庭時，亦可能發生利益衝突。

Source: Article 38(3) and 38(6) of the GDPR
資料來源：GDPR第38條第3項及第38條第6項

Tasks of the DPO
DPO之任務

---

11 What does 'monitoring compliance' mean?
何謂「監督法遵事宜」？

As part of these duties to monitor compliance, DPOs may, in particular:
具體而言，DPO得於監督法遵之職責範圍內：

- collect information to identify processing activities
  蒐集資訊以確認運用作業
- analyse and check the compliance of processing activities
  分析並檢視運用作業之法遵
- inform, advise and issue recommendations to the controller or the processor
  通知、勸告及提出建議予控管者或受託運用者

Source: Article 39(1)(b) of the GDPR
資料來源：GDPR第39條第1項第b款

12 Is the DPO personally responsible for non-compliance with data protection requirements?
DPO本人是否需為未遵循資料保護之要求負責？

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Data protection compliance is the responsibility of the controller or the processor.
不需要。DPO本人無須為未遵循資料保護之要求負責。應確保並得以證明依本規則執行運用者為控管者或受託運用者。資料保護法遵係控管者或受託運用者之責任。

13 What is the role of the DPO with respect to data protection impact assessments and records of processing activities?
DPO於個資保護影響評估及運用作業紀錄保存之角色為何？

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:
在個資保護影響評估方面，控管者或受託運用者應至少就以下事宜徵詢DPO之意見：

- whether or not to carry out a DPIA
  是否辦理DPIA
- what methodology to follow when carrying out a DPIA
  辦理DPIA應採取之方法

- whether to carry out the DPIA in-house or whether to outsource it
  DPIA應由組織內部辦理或委外辦理
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
  應採取何種安全措施（包含技術性及組織性措施）以降低當事人權利及利益之風險
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements
  個資保護影響評估是否依正確方式辦理，及其結論（是否於運用前辦理及採取何種安全措施）是否遵循資料保護要求

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.
在運用作業紀錄方面，係控管者或受託運用者應保留運用作業紀錄，而非DPO。然而，並未禁止控管者或受託運用者就其所負責之運用作業，指派DPO維護紀錄。該紀錄應視為使DPO得以執行其監督法遵、向控管者或受託運用者提供資訊及建議等任務的工具之一。

Source: Article 39(1)(c) and Article 30 of the GDPR
資料來源：GDPR第39條第1項第c款及第30條

Done in Brussels, on 13 December 2016
2016年12月13日於布魯塞爾完成

For the Working Party 工作小組
The Chairwoman 主席
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

2017年4月5日最新修訂並通過

For the Working Party 工作小組

The Chairwoman 主席

Isabelle FALQUE-PIERROTIN