ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

17/EN

WP 248 rev.01

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

關於第2016/679號規則(GDPR)中的個資保護影響評估（DPIA）以及確認運用是否「可能造成高風險」之指引

Adopted on 4 April 2017

2017年4月4日通過

As last Revised and Adopted on 4 October 2017

2017年10月4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條及第2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

由歐盟執委會司法總署第C署（基本權利和歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 03/075號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

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日通過之95/46/EC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

I. Introduction
導言

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA[2]), as does Directive 2016/680[3].

第2016/679[1]號規則（GDPR）將自2018年5月25日起施行。GDPR第35條導入了個資保護影響評估（DPIA[2]）之概念，如同第2016/680[3]號指令。

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance**.

DPIA是一種描述資料運用、評估運用之必要性及合比例性的程序，並透過評估及決定因應措施，協助控管者管理因運用個人資料[4]而對自然人權利和自由產生之風險。DPIA

[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).
2016年4月27日歐洲議會和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，制定第2016/679號規則（EU），並廢除第95/46/EC號指令（一般資料保護規則）。

[2] The term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.
於其他情形常使用之「隱私影響評估」（PIA）一詞概念相同。

[3] Article 27 of the 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, also states that a privacy impact assessment is needed for "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*".
2016年4月27日歐洲議會和歐盟理事會第2016/680號指令（EU）第27條關於權責機關為預防、調查、偵查或起訴刑事犯罪或執行刑事處罰而運用個人資料時，對自然人之保護與確保該資料之自由流通，亦指出若「*運用可能會對自然人之權利和自由造成高風險*」時，需進行隱私影響評估。

[4] The GDPR does not formally define the concept of a DPIA as such, but
GDPR並未正式定義DPIA本身之概念，然而

- its minimal content is specified by Article 35(7) as follows:
  依第35條第7項規定，其至少應包含以下內容：
  - "*(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;*
    「對預計運用作業和運用目的之系統性描述，於適用情形下，包含控管者尋求之合法利益；
  - *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes*
    與運用目的相關運用作業之必要性及合比例性之評估；
  - *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph*

是課責性的重要工具，因DPIA不僅可協助控管者遵守GDPR之要求，亦可使控管者證明已採取適當措施確保遵守本規則（請另參閱第24條）[5]。換言之，**DPIA是建立及證明合規性之程序**。

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever ishigher.

依據GDPR，不遵守DPIA之要求可能被權責監管機關處以罰鍰。當運用須辦理DPIA（第35條第1項和第3-4項）卻未辦理、未以正確方式辦理DPIA（第35條第2項和第7-9項）、或未依規定諮詢權責監管機關（第36條第3項第e款）時，可能被處以高達1千萬歐元之行政罰鍰，或於企業之情況下，最高可處前一會計年度全球年營業額之百分之二，以金額較高者為準。

II. Scope of the Guidelines
指引之範圍

These Guidelines take account of:

本指引依據：

1;and

第1項所述當事人權利和自由風險之評估；以及

- *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*

為因應風險而預計採行之措施，包含安全維護、安全措施和機制，以確保個人資料之保護，並在考量到當事人和其他相關人員之權利和合法利益之情況下證明對本規則之遵守」；

- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk*"

前言第84點已釐清其意義和角色如下：「*為強化本規則之遵循，當運用作業可能會對自然人之權利和自由造成高風險時，控管者應負責辦理個資保護影響評估，以檢視（尤其是）該風險之起源、性質、特殊性和嚴重性。*」

[5] See also recital 84: "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

請另參閱前言第84點：「*為證明個人資料之運用符合本規則，在決定應採行之適當措施時，評估結果應納入考量*」。

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP218[6];
  第29條個人資料保護工作小組（WP29）聲明，14/EN WP 218[6]；
- the WP29 Guidelines on Data Protection Officer 16/EN WP243[7];
  WP29個資保護長指引，16/EN WP 243[7]；
- the WP29 Opinion on Purpose limitation 13/EN WP203[8];
  WP29關於目的限制之意見，13 / EN WP 203[8]；
- international standards[9].
  國際標準[9]。

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by Data Protection Authorities (DPAs) under Article 35(4).
與體現於GDPR中之以風險為基礎的方法相符，DPIA並非對每個運用作業皆為強制性的。DPIA僅適用於當運用「*可能對自然人之權利和自由造成高風險*」時（第35條第1項）。為確保對強制辦理DPIA之情形作出一致解釋（第35條第3項），本指引首要目的即在於澄清此一概念，並為資料保護機關（DPAs）依據第35條第4項所應制定並公布須辦理DPIA的運用個資行為之清單提供標準。

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to

[6]WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532
14/EN WP 218，WP29於2014年5月30日通過關於資料保護法律架構下以風險為基礎的方法之作用聲明。
[7]WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A
16/EN WP 243，WP29於2016年12月13日通過關於個資保護長指引。
[8]WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409
13/EN WP 203，WP29於2013年4月2日通過第03/2013號關於目的之限制意見。
[9]e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).
例如 ISO 31000：2009，*風險管理 - 原則和指引*，國際標準化組織（ISO）; ISO / IEC 29134（項目），*資訊科技 - 安全技術 - 隱私影響評估 – 指引*，國際標準化組織（ISO）。

issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.

依據第70條第1項第e款，為鼓勵GDPR適用之一致性，歐洲個人資料保護委員會（EDPB）得發布指引、建議和最佳實務作法。本文件之目的係為EDPB未來之工作預先準備，從而澄清GDPR的相關規定，以協助控管者遵守法律，並為需要辦理DPIA之控管者提供法律確定性。

These Guidelines also seek to promote the development of:

本指引亦旨在促進下列事項之發展：

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
  歐盟通用之強制進行DPIA之運用作業清單（第35條第4項）；
- a common EU list of processing operations for which a DPIA is not necessary (Article35(5));
  歐盟通用之無需進行DPIA之運用作業清單（第35條第5項）；
- common criteria on the methodology for carrying out a DPIA (Article35(5));
  DPIA辦理方法之通用標準（第35條第5項）；
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
  具體指明何時應諮詢監管機關之通用標準（第36條第1項）；
- recommendations, where possible, building on the experience gained in EU Member States.
  在可能之情況下，借鑒歐盟成員國經驗做出之建議。

III. DPIA: the Regulation explained
DPIA：條文說明

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the “the risks of varying likelihood and severity for the rights and freedoms of natural persons” (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks[10] presented by the processing of personal data.

GDPR要求控管者採取適當措施以確保並能證明遵守GDPR，同時考量到「對自然人權利和自由造成各種可能和嚴重之風險」（第24條第1項）。控管者在某些情形下須辦理DPIA之義務應從其須適當管理個人資料運用風險[10]之一般義務的角度來理解。

A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.
「風險」是描述依據嚴重性和可能性進行估算的事件及其後果之可能情境。另一方面，「風險管理」可被定義為指導和控制組織中與風險相關之協調活動。

Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.
第35條係指「對個人之權利和自由」可能存在高風險之情況。如第29條個資保護工作小組關於風險基礎方法在資料保護法律架構中之作用的聲明所述，當事人之「權利和自由」主要考量的是資料保護和隱私之權利，然亦可能涉及其他基本權利，如言論自由、思想自由、行動自由、禁止歧視以及自由、良心和宗教之權利。

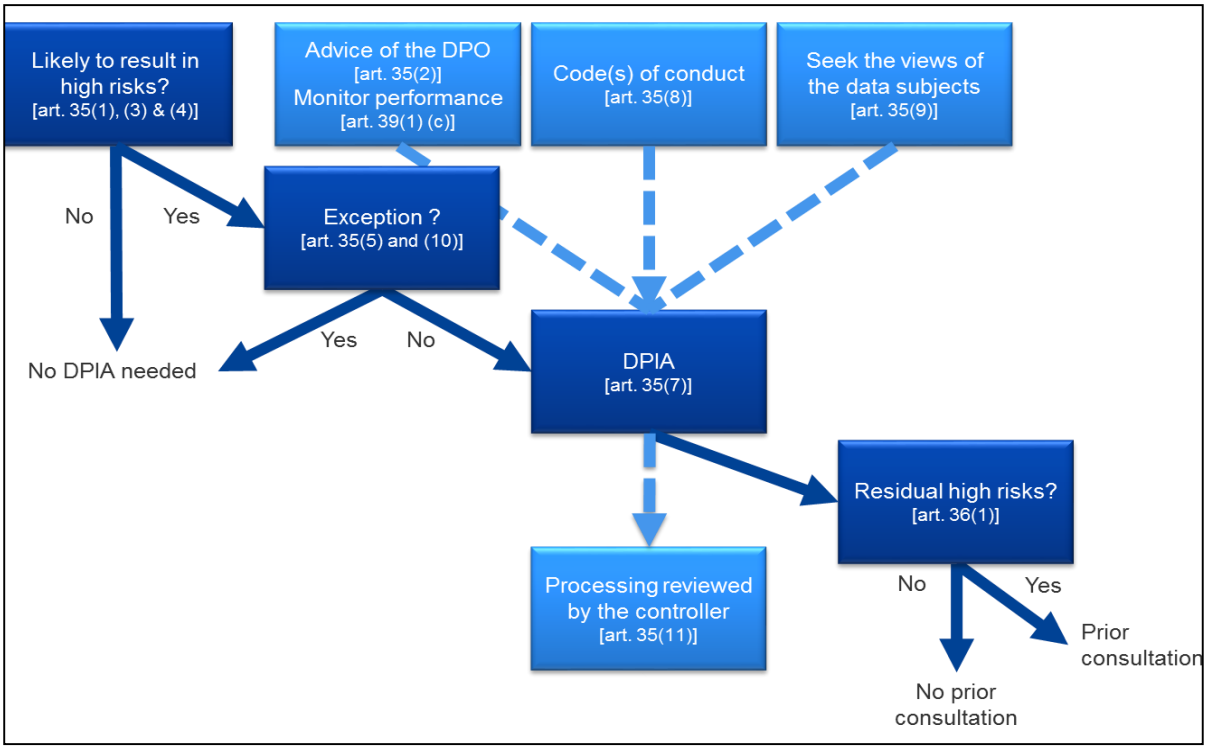
In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".
與體現於GDPR的風險基礎方法相符，DPIA並非對每個運用作業皆為強制性的。相反的，僅有當運用「可能對自然人之權利和自由造成高風險」時才需要DPIA（第35條第

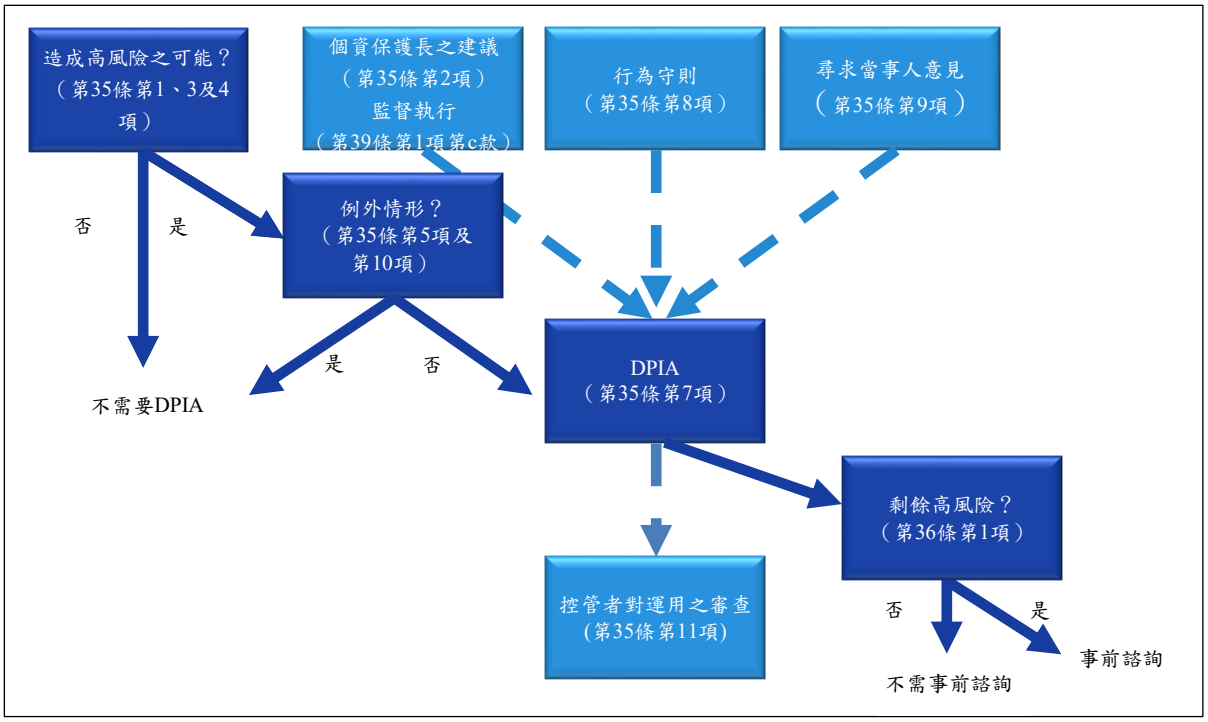
[10] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.
必須強調的是，為了管理自然人權利和自由之風險，必須辨識、分析、預估、評估、因應（例如減輕...）風險，並定期審查。控管者不得透過保險契約來規避風險管理之責任。

1項）。然而，未滿足觸發辦理DPIA義務之事實並不會減少控管者應實施對當事人權利和自由的適當風險管理措施之一般義務。在實務上，此意味著控管者必須不斷評估其運用活動所產生之風險，以確認何種類型之運用「可能對自然人權利和自由造成高風險」。

The following figure illustrates the basic principles related to the DPIA in the GDPR:

下圖說明GDPR中與DPIA相關之基本原則：





A. What does a DPIA address? A single processing operation or a set of similar processing operations.
DPIA著重點為何？單一運用作業或一系列類似運用作業。

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks"*. Recital 92 adds that *"there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

DPIA可僅涉及單一資料運用作業。然而，第35條第1項規定「*單一評估可針對一系列類似且呈現相似高風險之運用作業*」。前言第92點補充說明「*在某些情況下，個資保護影響評估之標的不限於單一計畫，是屬較合理且經濟的，例如，當公務機關或機構欲建立共同的應用程式或運用平台，或當數個控管者計畫引進共同的應用程式或跨產業或跨界之運用環境，或為廣泛使用的水平整合活動*」。

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

一份DPIA可用於評估在性質、範圍、背景、目的和風險方面**類似之數個運用作業**。實際上，DPIA旨在系統性的研究對自然人權利和自由可能造成高風險之新情況，因此對已經研究過的案例（例如在特定情況和特定目的下進行之運用作業）即無辦理DPIA之必要性。此種情況可能係使用類似之技術並基於相同之目的蒐集相同種類之資料。例

如，當市政當局的各機關獨自建立類似之CCTV系統時，可辦理一份DPIA，涵蓋不同控管者的運用作業，或是鐵路運營商（單一控管者）可在一份DPIA中涵蓋其所有車站的影音監視。此亦可能適用於由不同資料控管者實施類似運用作業之情形。於此情況下，所提供之DPIA應被共享或可公開取得，於DPIA中所描述之措施必須執行，且須提供僅辦理單一DPIA之正當理由。

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

當運用作業涉及共同控管者時，需精確地定義其各自之義務。DPIA中應指明哪一方負責處理風險及保護當事人權利和自由之各種措施。每個資料控管者皆應於未洩露秘密（例如：保護營業秘密、智慧財產權，商業機密資訊）或揭露弱點之情況下，表達其需求並分享有用資訊。

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

當技術產品（例如硬體或軟體產品）可能由不同的資料控管者進行不同運用作業時，**使用DPIA評估其對資料保護之影響亦有用處**。當然，使用該產品之資料控管者仍有義務關於該特定執行自行辦理DPIA，但可於適當情形下使用由產品供應商準備之DPIA。智能電錶製造商和公用事業公司間之關係可提供示例。每個產品提供者或受託運用者應共享有用資訊，但不至洩露秘密，亦不至因揭露弱點導致安全風險。

B. Which processing operations are subject to a DPIA? Apart from exceptions, where they are "*likely to result in a high risk*".
哪些運用作業須辦理DPIA？除例外情形，當運用「*可能造成高風險*」時。

This section describes when a DPIA is mandatory, and when it is not necessary to carry out a DPIA.
本章節描述何時DPIA為強制性的，以及何時不需辦理DPIA。

Unless the processing operation meets an exception (III.B.a), a DPIA has to be carried out where a processing operation is "*likely to result in a high risk*" (III.B.b).
除非運用作業符合例外情形（III.B.a），否則當運用作業「*可能造成高風險*」時，即必須辦理DPIA（III.B.b）。

a） When is a DPIA mandatory? When processing is "*likely to result in a highrisk*".
何時DPIA為強制性的？當運用「*可能造成高風險*」時。

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[11].
GDPR並未要求每個可能造成自然人權利和自由風險之運用作業皆需辦理DPIA。只有當運用「*可能對自然人權利和自由造成高風險*」之情況下才必須強制辦理DPIA（第35條第1項，第35條第3項加以闡明，並由第35條第4項補充）。此規定在引入新的資料運用技術時尤為重要[11]。

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.
若不確定是否需辦理DPIA，WP29建議仍辦理DPIA，因DPIA係協助控管者遵守資料保護法的有效工具。

Even though a DPIA could be required in other circumstances, Article 35(3) provides some

[11] See recitals 89, 91 and Article 35(1) and (3) for further examples.
有關進一步示例，請參閱前言第89點和第91點以及第35條第1項和第3項。

examples when a processing operation is "*likely to result in high risks*":
儘管在其他情狀下仍可能需要DPIA，第35條第3項提供了當運用作業「*可能造成高風險*」的一些示例：

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the naturalperson*[12]*;*
  (a) 基於自動化運用（包含剖析）對與自然人相關之個人面向進行系統性和廣泛性的評估，且基於該評估所作成之決策將對自然人產生法律效果或類似重大影響[12]*；*
- *(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*[13]*;or*
  (b)大規模的運用第9條第1項規定之特種資料，或第10條所規定之與刑事前科及犯罪相關之個人資料[13]*；或*
- *(c) a systematic monitoring of a publicly accessible area on a largescale*".
  (c)於公眾開放區域進行大規模之系統性監控。

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.
如GDPR第35條第3項序文使用「*特別地*」一詞所示，此為例示清單，可能存在未列於清單但具有類似高風險之「高風險」運用作業，這些運用作業亦應受DPIA之約束。基於此原因，下文訂定之標準有時會超出GDPR第35條第3項提供的三個示例的理解範圍。

In order to provide a more concrete set of processing operations that require a DPIA due to

[12]See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".
請參閱前言第71點：「*尤其是分析或預測有關工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、位置或行動等面向，以建立或使用個人剖析*」。
[13] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".
請參閱前言第75點：「*當個人資料運用涉及揭露種族或人種、政治意見、宗教或哲學信仰、工會會員、以及基因資料之運用、有關健康之資料或有關性生活或前科及犯罪或相關安全措施之資料時*」。

their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processing operations[14], the following nine criteria should be considered.

為了提供一套因其固有之高風險而需辦理DPIA之更具體的運用作業，並考量到第35條第1項和第35條第3項第a至c款之特定要件、第35條第4項和前言第71、75和91點應於國家層級制定之清單、以及其他GDPR規範所提及「*可能造成高風險*」之運用作業[14]，應考量以下九項標準。

1. Evaluation or scoring, including profiling and predicting, especially from "*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements*" (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

   評估或評分，包含剖析和預測，尤其是「*關於當事人工作表現、經濟狀況、健康、個人偏好或興趣、可信度或行為、位置或行動等面向*」（前言第71和91點）。此類情形之示例可包含金融機構依據信用參考資料庫或反洗錢和反恐融資（AML / CTF）或詐欺資料庫篩選其客戶，或是一家直接向消費者提供基因測試的生物科技公司，以評估和預測疾病/健康風險，亦或以網站使用或導覽建立行為或行銷剖析之公司。

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.

   具有法律效果或類似重大影響之自動化決策：當運用目的是為做出有關當事人之決定，且該決定產生「*關於該自然人之法律效果*」或該決定「*類似重大影響*

[14] See e.g. recitals 75, 76, 92, 116.
請參閱如前言第75、76、92、116點。

該自然人」（第35條第3項第a款）。例如，運用可能導致對個人之排除或歧視。若運用對個人影響甚微或沒有影響則與此特定標準不符。與此概念相關之進一步說明將規範於WP29的剖析指引。

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[15]. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
系統性監控：用於觀察、監測或控制當事人之運用，包括透過網路蒐集之資料或「*於公眾開放區域進行系統性之監控*」（第35條第3項第c款）[15]。此類型之監控會成為一項判斷標準，係因蒐集個人資料時，當事人可能無法得知蒐集者為何人以及其資料將如何被使用。此外，當事人在公開場所（或公眾開放區域）可能無法避免此類運用。

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked

[15]The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):
WP29對「系統性」之解釋，係以下一項或多項情形（請參閱WP29個資保護長指引 16/EN WP 243）：
- 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。

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.
WP29將「*公眾得接近使用區域*」解釋為對任何大眾開放之任何場所，例如廣場、購物中心、街道、市場、火車站或公共圖書館。

to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

敏感資料或高度私人性質資料：此類資料包括第9條定義之特殊類型個人資料（例如有關個人政治觀點之資訊），及與第10條定義之前科或犯罪相關個人資料。例如綜合醫院保存病人醫療記錄或私人調查員保留違法者之詳細資訊。除GDPR這些規定外，某些類型之資料被視為會對個人權利和自由增加可能的風險。這些個人資料會被認為是敏感的（如同通常對於"敏感"之理解），因其與家庭和私人活動相關聯（如電子通訊秘密應受保護），或因其影響基本權利之行使（如蒐集所在位置之資料會造成自由移動權利之質疑），或因其違反明顯對當事人日常生活造成嚴重影響（如金融資料可能被用於支付詐欺）。在此情況下，資料是否已由當事人或第三方公開是有關聯性的。若預期資料將為某些目的之進一步運用，則可將個人資料已公開之事實視為評估的要素之一。此標準亦可包括諸如個人文件、電子郵件、日記、有筆記記錄功能電子閱讀器中之筆記以及生活日誌應用程式中所包含非常私人之資訊。

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a largescale[16]:

   大規模資料運用：雖然前言第91點提供了一些指導，GDPR並未定義構成大規模之要件。無論如何，WP29建議在決定是否進行大規模運用時，應特別考量以下要素[16]:

   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

[16]See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
請參閱WP29個資保護長指引，16/EN WP 243。

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；

b. 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；

c. the duration, or permanence, of the data processing activity;
資料運用作業之期間或持續性；

d. the geographical extent of the processing activity.
運用作業之地理涵蓋範圍。

6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the datasubject[17].
配對或組合資料集：例如源自為不同目的和/或由不同資料控管者實施的兩個或兩個以上的資料運用作業，且其方式將超出當事人之合理期待[17]。

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, *etc*.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
與弱勢當事人相關之資料（前言第75點）：運用此類型資料之所以成為一項判斷標準，係因其增加當事人和資料控管者間之權力失衡，此意味著當事人可能無法輕易地同意或拒絕其個人資料之運用或行使其權利。弱勢當事人可能包含兒童（兒童可能被認為無法有意識地和深思熟慮地拒絕或同意對其資料之運用）、員工、較弱勢需特殊保護之群體（精神病患者、尋求庇護者或老年人、病患等），以及在任何情況下，會認為當事人與控管者間的關係產生失衡之情事。

8. Innovative use or applying new technological or organisational solutions, like

[17]See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.
請參閱WP29關於目的限制意見中之說明，13/EN WP 203，第24頁。

combining use of finger print and face recognition for improved physical access control, *etc*. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

創新使用或應用新的技術性或組織性之解決方案，例如結合使用指紋和臉部辨識以改進實體存取控制等。GDPR明確指出（第35條第1項及前言第89點和第91點），使用「*依照現有的技術知識狀態*」（前言第91點）定義下之新技術可觸發辦理DPIA之要求。這是因為使用此類技術會涉及新形式之資料蒐集和使用，並可能對個人之權利和自由產生高風險。實際上，新技術的使用對個人和社會之後果可能是未知的。DPIA將可協助資料控管者理解和處理此類風險。例如，某些「物聯網」(IoT) 應用程式可能會對個人的日常生活和隱私造成重大影響；因此需要DPIA。

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

   當運用本身「*阻止當事人行使權利或使用服務或契約*」時（第22條和前言第91點）。此情形包括目的在允許、變更或拒絕當事人取得服務或簽訂契約之運用作業。例如銀行依據信用參考資料庫篩選其客戶，以決定是否提供貸款。

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

在多數情況下，當運用符合上述兩項標準時，資料控管者會認為須辦理DPIA。一般而

言，WP29認為當運用符合越多項標準時，越有可能對當事人之權利和自由造成高風險，因此需要DPIA，無論控管者預計採行之措施為何。

However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.
然而，在某些情況下，資料控管者可認為即使運用僅符合其中一項標準亦須辦理DPIA。

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:
以下示例說明如何使用這些標準來評估一個特定的運用作業是否需要DPIA：

Examples of processing **運用之示例**	**Possible Relevant criteria** **可能的相關標準**	**DPIA likely to be required?** **是否可能需要DPIA？**
A hospital processing its patients' genetic and health data (hospital information system). 醫院運用病患之基因和健康資料（醫院資訊系統）。	- Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。 - Data processed on a large-scale. 大規模資料運用。	Yes 是
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates. 使用攝影系統監控高速公路上的駕駛行為。控管者預計使用智能影像分析系統來挑選車輛並自動識別車牌。	- Systematic monitoring. 系統性監控。 - Innovative use or applying technological or organisational solutions. 創新使用或應用技術性或組織性之解決方案	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station,	- Systematic monitoring. 系統性監控。 - Data concerning vulnerable data subjects.	

internet activity, *etc*. 公司系統性地監控員工活動，包括監控員工的個人工作區、網路活動等。	與弱勢當事人相關之資料。	
The gathering of public social media data for generating profiles. 蒐集公眾社交媒體資料以建立剖析檔案。	- Evaluation or scoring. 評估或評分。 - Data processed on a largescale. 大規模資料運用。 - Matching or combining of datasets. 配對或組合資料集。 - Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。	
An institution creating a national level credit rating or fraud database. 建立國家層級的信用等級或詐欺資料庫之機構。	- Evaluation or scoring. 評估或評分。 - Automated decision making with legal or similar significant effect. 具有法律效果或類似重大影響之自動化決策。 - Prevents data subject from exercising a right or using a service or a contract. 阻止當事人行使權利或使用服務或契約。 - Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質資料。	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials 基於歸檔目的，儲存用於研究計畫或臨床試驗之弱勢當事人的假名化個人敏感資料。	- Sensitive data. 敏感資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。 - Prevents data subjects from exercising a right or using a service or a contract. 阻止當事人行使權利或使用服務或契約。	

Examples of processing **運用之示例**	**Possible Relevant criteria** **可能的相關標準**	**DPIA likely to be required?** **是否可能需要DPIA？**
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91). 由「個別醫生、其他健康照護專業人員或律師」運用「病患或客戶之個人資料」（前言第91點）。	- Sensitive data or data of a highly personal nature. 敏感資料或高度私人性質之資料。 - Data concerning vulnerable data subjects. 與弱勢當事人相關之資料。	No 否
An online magazine using a mailing list to send a generic daily digest to its subscribers. 網路雜誌使用寄件清單向其訂閱戶發送一般每日摘要。	- Data processed on a largescale. 大規模資料運用。	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website. 電子商務網站以在其網站上查看或購買項目的有限剖析，廣告其最佳汽車零件。	- Evaluation or scoring. 評估或評分。	

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.
反之，運用作業可能符合上述情況，但控管者仍認為「不太可能造成高風險」。在此情況下，控管者應證明並記錄不辦理DPIA之原因，且應包含/記錄個資保護長之意見。

In addition, as part of the accountability principle, every data controller "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

此外，作為課責原則的一部分，每個資料控管者「*應保有於其職責範圍內運用活動之記錄*」，除其他事項外，包含運用目的、資料類型和資料接收者之描述，以及「*如適用，第32條第1項所述技術性和組織性安全措施之一般說明*」（第30條第1項），並且必須評估是否存在高風險之可能，即使控管者最終決定不辦理DPIA。

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[18]. The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article35(4).

備註：監管機關被要求建立、公開並向EDPB溝通需要DPIA的運用作業清單（第35條第4項）[18]。上述之標準可協助監管機關建立該清單，並在適當時機添加更具體之內容。例如，任何類型的生物特徵資料或兒童資料之運用亦可被視為與依據第35條第4項建立之清單相關聯。

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

   何時不需要DPIA？當運用不太「*可能造成高風險*」或已存在類似之DPIA時，又或該運用是在2018年5月之前獲得授權、或其具有法律依據，或是在不需要DPIA之運用作業清單中。

WP29 considers that a DPIA is not required in the following cases:

[18]In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

在此背景下「*當此類型清單涉及與向當事人提供商品或服務或於數個成員國監控其行為相關之運用活動，或對歐盟境內個人資料的自由流通產生實質性影響時，權責監管機關應適用第63條所述之一致性機制*」（第35條第6項）。

WP29認為在下列情況下不需要DPIA：

- **where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons"** (Article 35(1));
  當運用不太「可能對自然人權利和自由造成高風險」時（第35條第1項）；
- **when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.** In such cases, results of DPIA for similar processing can be used (Article35(1)[19]);
  當運用之性質、範圍、背景和目的與已辦理之DPIA非常相似時。在此情形下，可使用類似運用之DPIA的結果（第35條第1項[19]）；
- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed[20] (see III.C);
  在未改變特定條件下，當監管機關已於2018年5月前檢查過運用作業時[20]（請參閱III.C）；
- **where a processing operation,** pursuant to point (c) or (e) of article 6(1), **has a legal basis** in EU or Member State law, where the law regulates the specific processing operation **and where a DPIA has already been carried out** as part of the establishment of that legal basis (Article 35(10))[21], except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;
  當依據第6條第1項第c款或第e款之**運用作業**在歐盟或成員國法律中**具有法律依據**，該法律規範了具體運用作業**且已辦竣之DPIA已**作為建構該法律依據之一部分時（第35條第10項）[21]，除非成員國已聲明有必要於運用活動前辦理DPIA；
- **where the processing is included on the optional list (established by the**

[19]"*A single assessment may address a set of similar processing operations that present similar high risks.*"
「單一評估得針對一系列呈現相似高風險之類似運用作業」。

[20] "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).
「執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效」（前言第171點）。

[21]When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities.
若係為提供運用之法律依據而在立法階段辦理之DPIA，則可能需要在開始作業前再次檢視，因通過之法規可能會與提案不同，而影響到隱私權及資料保護議題。此外，即使有DPIA，在法規通過時也可能無法對實際運用提供足夠之技術細節描述。在此情況下，於執行實際運用作業前可能仍需辦理特定之DPIA。

supervisory authority) of processing operations for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, *etc*. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with all the relevant requirements of the GDPR.

當運用列於無需DPIA的運用作業選擇性清單（由監管機關建立）中（第35條第5項）。此類清單可能包含應符合該機關指定條件之運用活動，特別是透過指引、特定決策或授權、合規性規則等（例如法國制度下的授權、免責、簡化規則、合規性包裹...）。在此情況下，由權責監管機關重新評估，不需要DPIA，但前提為運用需嚴格屬於該清單中提及之相關程序範圍，並持續完全符合所有GDPR相關要求。

C. What about already existing processing operations? DPIAs are required in some circumstances.

對於現行運用作業之要求為何？在某些情況下需要DPIA。

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

當現行的運用作業可能對自然人之權利和自由造成高風險；及將運用之性質、範圍、背景和目的納入考量時，該風險已發生變化，應辦理DPIA。

A DPIA is not needed for processing operations that have been checked by a supervisory authority or the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

監管機關或個資保護長已依據95/46/EC指令第20條檢視之運用作業，且這些運用作業之實施方式自先前檢視後並未改變者，無須辦理DPIA。實際上，「*執委會通過之決定及監管機關依95/46/EC指令所為之授權，於修正、取代或廢止前仍繼續有效*」（前言第171點）。

Conversely, this means that any data processing whose conditions of implementation (scope,

purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

相反的，此意味著當任何資料運用之實施條件（範圍、目的、蒐集之個人資料、資料控管者或接收者之身分、資料留存期、技術性和組織性措施等）自監管機關或個資保護長先前檢查以來已發生變化，且可能造成高風險時，則該運用應辦理DPIA。

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations[22], for example because a new technology has come into use or because personal data is being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned.

此外，在運用作業造成之風險有變化後，可能需要DPIA[22]，例如因新技術之使用或因個人資料被用於其他不同目的。資料運用作業可能快速發展，因而可能出現新的弱點。因此，應注意者為，DPIA之修正不僅有助於持續改進，且對於在不斷變化的環境中保持資料保護水準亦至關重要。當運用作業之組織或社會背景改變時，DPIA也可能變得必要，例如，因某些自動決策之影響變得更加重大，或新的當事人類型變得容易受到歧視。上述每一種示例都可能是導致相關運用作業產生風險變化之要素。

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

相反的，某些變化也可能降低風險。例如，運用作業可逐步發展使決策不再自動化或監控活動不再為系統性的。在此情況下，對風險分析之審查可表明不再需要辦理DPIA。

[22]In terms of the context, the data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats, *etc.*), security measures and international transfers.

背景係指蒐集之資料、目的、功能、運用之個人資料、接收者、資料組合、風險（支援資產、風險來源、潛在影響、威脅等）、安全措施和國際傳輸等方面。

As a matter of good practice, **a DPIA should be continuously reviewed and regularly re-assessed.** Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

作為優良實務做法，**應持續審查DPIA並定期對其進行重新評估。**因此，即使在2018年5月25日時不需要DPIA，作為一般性課責義務之一部分，控管者亦必須在適當之時間點辦理DPIA。

D. How to carry out a DPIA?
如何辦理DPIA？

a) At what moment should a DPIA be carried out? Prior to the processing.
應於何時辦理DPIA？在運用資料之前。

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93)[23]. This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

DPIA應在「*運用前*」（第35條第1項和第35條第10項及前言第90點和第93點）[23]辦理。此與資料保護設計（by design）和預設（by default）原則一致（第25條和前言第78點）。應將DPIA視為協助相關運用的決策工具。

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

在運用作業的設計中應儘早啟動DPIA，即使某些運用作業仍屬未知。在整個運用作業期間，定期更新DPIA將確保資料保護和隱私納入考量，並將鼓勵建立促進合規性之解決方案。隨著開發過程之進展，亦可能需要重複評估中的個別步驟，因某些技術性或組織性措施之選擇可能會影響運用所造成風險之嚴重性或可能性。

The fact that the DPIA may need to be updated once the processing has actually started is not

[23] Except when it is an already existing processing that has been prior checked by the Supervisory Authority, in which case the DPIA should be carried out before undergoing significant changes.
除非是監管機關先前已檢查過之現行運用，否則於進行重大變更前，應辦理DPIA。

a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. **Carrying out a DPIA is a continual process, not a one-time exercise**.

一旦運用開始實際實施，可能需要更新DPIA之事實不是延遲或不辦理DPIA的正當理由。DPIA是一種持續進行的程序，尤其是當運用作業是處於動態且不斷變化之情況下。**辦理DPIA是一種持續之程序，而非一次性作為。**

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors.
誰有義務辦理DPIA？控管者，及其DPO和受託運用者。

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.
控管者需負責確保辦理DPIA（第35條第2項）。DPIA可以由組織內部或外部其他人員完成，然對該任務之最終責任仍歸屬於控管者。

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
當依規定指定DPO時（第35條第2項），**控管者亦須尋求個資保護長（DPO）之建議**，DPO之建議以及控管者之決定應記錄於DPIA中。DPO亦應監督DPIA之辦理成效（第39條第1項第c款）。16/EN WP 243，WP29個資保護長指引提供了進一步的指導。

If the processing is wholly or partly performed by a data processor, **the processor should assist the controller in carrying out the DPIA** and provide any necessary information (in line with Article 28(3)(f)).
若運用之全部或一部係由資料受託運用者實施，則**受託運用者應協助控管者辦理DPIA**，並提供任何必要之資訊（符合第28條第3項第f款）。

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:
「*適當時*」，控管者必須「*尋求當事人或其代理人之意見*」（第35條第9項）。WP29認為：

- those views could be sought through a variety of means, depending on the context (e.g.

a generic study related to the purpose and means of the processing operation, a question to the staff representatives, or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;
可透過各種方式尋求該意見，取決於具體情況（例如，與運用作業目的和方式有關之一般性研究、向員工代表提出之問題、或發送通常的意見調查予資料控管者未來客戶）以確保控管者有法律依據運用尋求此類意見所涉及之任何個人資料。然應指出，同意運用顯然不是尋求當事人意見的一種方式；

- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
若資料控管者的最終決定與當事人之意見不同時，應記錄其繼續實施或停止實施之原因；

- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.
若控管者認為不適合尋求當事人意見，亦應紀錄其理由，例如，將損害公司業務計畫之機密性，或是不符合比例性或是不可實行的。

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:
最後，作為一種良好實務做法，應依據內部政策、程序和規則，定義並記錄其他特定角色和職責，例如：

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the DPIA validation process;
當特定業務單位建議辦理DPIA，該單位應就DPIA提供意見，並參與DPIA確認程序；

- where appropriate, it is recommended to seek the advice from independent experts of different professions[24] (lawyers, IT experts, security experts, sociologists, ethics, *etc*.).
在適當情況下，建議諮詢不同專業的獨立專家[24]（律師、IT專家、安全專家、社

[24]*Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.
對歐盟隱私影響評估架構之建議，Deliverable D3:http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

會學家、倫理學家等）之意見。

- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article28(3)(f));
  受託運用者之角色和職責必須以合約規定；且DPIA必須在受託運用者之協助下辦理，同時考量運用之性質和受託運用者可得之資訊（第28條第3項第f款）；
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
  若有指定首席資訊安全長（CISO），其與DPO可建議控管者對特定之運用作業辦理DPIA，並應協助利害關係人導入方法論、協助鑑定風險評估品質以及剩餘風險之可接受性，並針對資料控管者背景建構相關知識；
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.
  若有指定首席資訊安全長（CISO），其和/或IT部門，應提供控管者協助，並可依據安全或營運需要，建議對特定運用作業辦理DPIA。

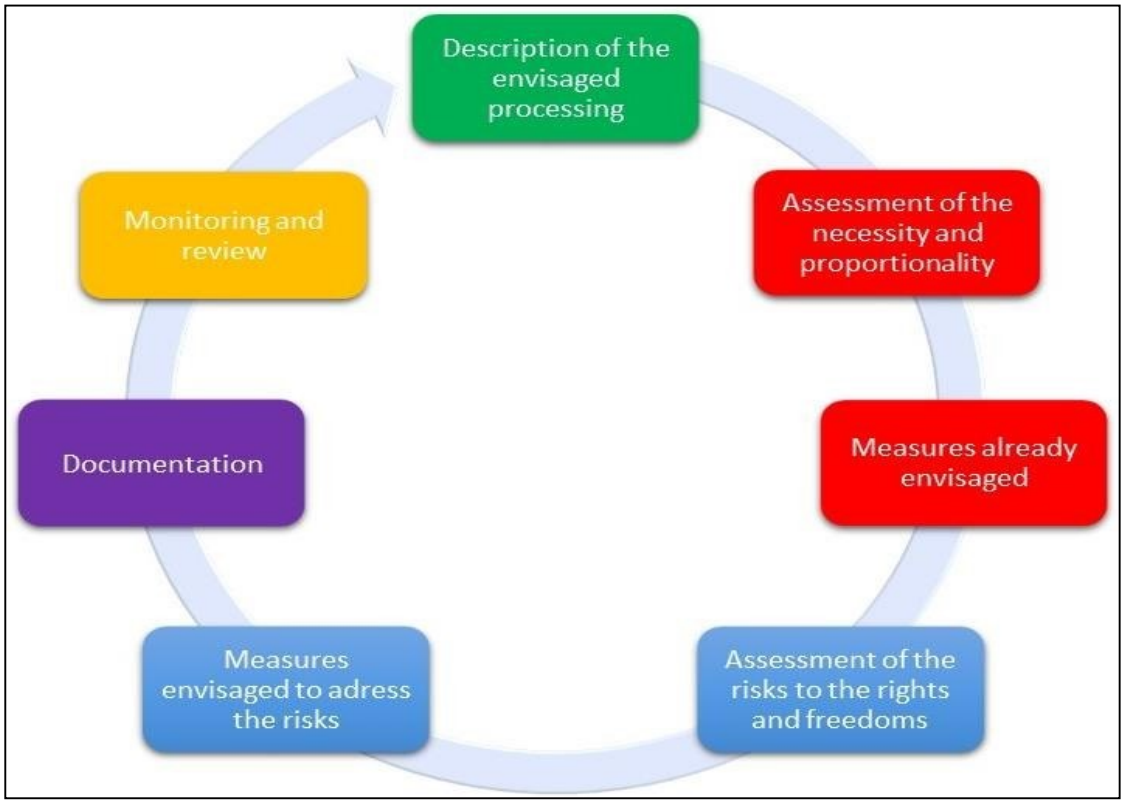
c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.
辦理DPIA之方法論為何？不同之方法論，但共同之標準。

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):
GDPR規定了DPIA至少應包含之要件（第35條第7項，及前言第84點和第90點）：

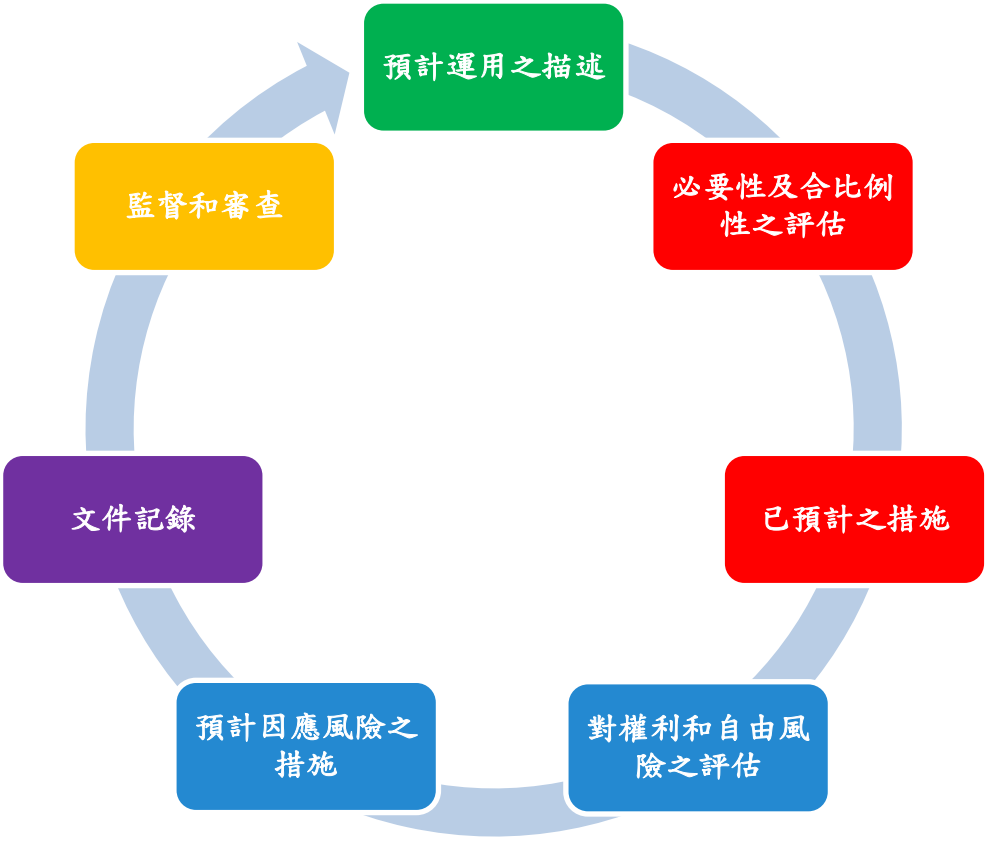
- *"a description of the envisaged processing operations and the purposes of the processing";*
  「預計運用作業和運用目的之描述」；
- *"an assessment of the necessity and proportionality of the processing";*
  「運用之必要性及合比例性之評估」；
- *"an assessment of the risks to the rights and freedoms of data subjects";*
  「對當事人權利和自由風險之評估」；

- *"the measures envisaged to:*
  「預計採取之措施：
  - *"address the risks";*
    「以因應風險」；
  - *"demonstrate compliance with this Regulation".*
    「以證明遵守本規則」

The following figure illustrates the generic iterative process for carrying out a DPIA[25]:
下圖說明辦理DPIA的一般重複循環程序[25]：



[25]It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.
必須強調，此處描述之程序是重複循環性的：實際上，很可能在DPIA完成前需多次重複進行各個階段。



Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.

在評估資料運用作業之影響時，必須考量（第35條第8項）行為守則（第40條）之遵守。若行為守則適用於運用作業，則可用於證明已選擇或實施適當之措施。亦應考量用以證明控管者和受託運用者遵守GDPR運用作業之認證、標章和標誌（第42條），以及具有約束力之企業守則（BCR）。

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. The DPIA implementation is therefore scalable. This means that even a

small data controller can design and implement a DPIA that is suitable for their processing operations.

GDPR中所有相關要求為設計和辦理DPIA提供了廣泛性的通用架構。DPIA的實際辦理將取決於GDPR之要求，並可透過更詳盡的實務指導進行補充。因此，DPIA之辦理是可延展的。此意味著即使是小規模的資料控管者亦可設計和辦理適合其運用作業之DPIA。

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well- defined components of risk management (e.g. ISO 31000[26]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following processes, by:

GDPR前言第90點概述了DPIA所需之各項構成要素，這些構成要素與風險管理（例如ISO 31000[26]）明確定義之構成要素重疊。以風險管理術語來說，DPIA旨在透過以下程序「管理」自然人之權利和自由「風險」：

- establishing the context: "taking into account the nature, scope, context and purposes of the processing and the sources of the risk";
  建立背景：「將運用之性質、範圍、背景和目的以及風險來源納入考量」；
- assessing the risks: "assess the particular likelihood and severity of the high risk";
  評估風險：「評估高風險之特殊可能性和嚴重性」；
- treating the risks: "mitigating that risk" and "ensuring the protection of personal data", and "demonstrating compliance with this Regulation".
  因應風險：「降低風險」和「確保個人資料之保護」，以及「證明遵守本規則」。

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security). Conversely, risk management in other fields (e.g. information security) is focused on the organization.

備註：GDPR下之DPIA是一種管理當事人權利風險之工具，因此如同在某些領域（例如社會安全）之情況，需採取當事人觀點。反之，其他領域之風險管理（例如資訊安全）則著重於組織面。

[26]Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).
風險管理程序：溝通和諮詢、建立背景、風險評估、風險處理、監控和審查（請參閱ISO 31000預先審查中之條款和定義，及目錄）：https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

GDPR提供資料控管者決定DPIA結構和形式之彈性，以便與現有的工作實務相互配合。歐盟和全世界有許多不同的既定程序，皆考量到前言第90點中所描述之構成要素。然而，無論其形式為何，DPIA必須是對風險的真正評估，允許控管者對該風險採取因應措施。

Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR. In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. **It is up to the data controller to choose a methodology, but this methodology should be compliant with the criteria provided in Annex2**.

可使用不同之方法論（請參閱附錄1資料保護和隱私影響評估方法論示例）來協助執行GDPR中規定之基本要求。為允許這些不同方法存在，同時使控管者得以遵守GDPR之規範，因此列出共同標準（請參閱附錄2）。其釐清本規則之基本要求，但為不同的執行模式提供足夠的空間。這些標準可用於證明特定的DPIA方法論符合GDPR要求之標準。**雖然是由資料控管者選擇方法論，但該方法論應符合附錄2中提供之標準。**

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.

WP29鼓勵發展特定部門(sector-specific)的DPIA架構。因可利用特定之部門知識，使DPIA得因應特定類型運用作業之細節（例如：特定類型之資料、公司資產、潛在影響、威脅、措施）。此意味著DPIA可因應特定經濟部門，或使用特定技術或實施特定類型之運用作業時所出現之問題。

Finally, where necessary, "*the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation*" (Article 35(11)[27]).
最後，在必要時，「*控管者應至少於運用作業所造成之風險發生變化時，審查評估運用之實施是否符合個資保護影響評估*」（第35條第11項[27]）。

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.
是否有義務公布DPIA？沒有，但公布摘要內容可促進信任，且若因事先諮詢或DPA之要求，則必須將完整的DPIA提供予監管機關。

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.
公布DPIA並非GDPR之法律要求，而係控管者之決定。然而，控管者應考量至少公布部分內容，例如DPIA之摘要或結論。

The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.
該程序之目的可能是在協助促進對控管者運用作業之信任，並展現其課責性和透明化。當大眾受到運用作業影響時，公布DPIA是一種非常良好的實務範例。特別是在政府機關辦理DPIA之情況下。

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.
公布之DPIA不需包含整份評估文件，特別是當DPIA可能涉及有關資料控管者安全風險之特定資訊或洩露商業機密或商業敏感資訊時。在此情況下，公布的版本可僅包含DPIA主要評估結果之摘要，或甚至僅為已辦理DPIA之聲明。

Moreover, where a DPIA reveals high residual risks, the data controller will be required to

[27] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.
第35條第10項明確排除第35條第1至7項之適用。

seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice[28], and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents.

此外，當DPIA顯示高剩餘風險時，資料控管者將被要求事先諮詢監管機關對該運用之意見（第36條第1項）。在此情況下，必須完整提供DPIA（第36條第3項第e款）。依據各會員國於公開取得官方文件之原則，監管機關得提供建議[28]，且不會損害商業秘密或揭露安全漏洞。

E. When shall the supervisory authority be consulted? When the residual risks are high.
何時應諮詢監管機關？當有高剩餘風險時。

As explained above:
如上所述：

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
  當運用作業「*可能對自然人權利和自由造成高風險*」時，需要DPIA（第35條第1項，請參閱III.B.a）。例如，大規模運用健康資料被認為可能造成高風險，並且需要DPIA；
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[29] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, *etc*.) in addition to existing policies (notice, consent, right of access, right to object, *etc*.).
  因此，資料控管者有責任評估當事人權利和自由之風險，並確認可將此些風險

[28] Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2).
只有當監管機關認為預計之運用不符合第36條第2項規定之規定時，才需向控管者提出書面建議。

降低至可接受程度之預計措施[29]及證明遵守GDPR（第35條第7項，請參閱III.C.c）。例如除現有政策外（通知、同意、近用權、拒絕權等），在筆記型電腦上儲存個人資料時，使用適當的技術性和組織性安全措施（有效全硬碟加密、堅實金鑰管理、適當存取控制、安全備份等）。

In the laptop example above, if the risks have been considered as sufficiently reduced by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) that the data controller must consult the supervisory authority.
在上述筆記型電腦示例中，若資料控管者認為風險已充分降低，並於考量第36條第1項和前言第84點和第94點後，則可在不諮詢監管機關之情況下實施運用。若資料控管者無法充分因應已確認之風險（即剩餘風險仍維持高風險時），資料控管者必須諮詢監管機關。

An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well- known vulnerability is not patched).
無法接受之高剩餘風險的示例包括對當事人可能造成重大甚至無法回復之後果（例如：非法存取資料導致當事人受到生命威脅、裁員、財務危機）和/或當風險似乎明顯會發生時（例如：由於其共享、使用或散布模式以至無法減少造訪資料人數，或尚未修補已知之漏洞）。

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required[30].
若資料控管者找不出足以將風險降低至可接受程度之措施時（即仍維持高剩餘風險時），則需諮詢監管機關[30]。

[29]Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).
包括考量EDPB和監管機關現有之指導，並考量第35條第1項規定的最新技術和實施成本。
[30] Note: "*pseudonymization and encryption of personal data*" (as well as data minimization, oversight mechanisms, *etc*.) are not necessarily appropriate measures. They are only examples. Appropriate measures depend on the context and the risks, specific to the processing operations.
備註：「*個人資料之假名化和加密*」（以及資料最小化、監督機制等）不一定為適當之措施。僅可做為示例。適當措施取決於運用作業之背景和風險。

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

此外，若成員國法律要求，當控管者實施之運用涉及公共利益時，包括與社會保護和公共衛生相關之運用，控管者必須就該運用諮詢監管機關，和/或得到監管機關事先授權（第36條第5項），則控管者必須諮詢監管機關。

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

但仍應說明，無論是否需要依據剩餘風險程度諮詢監管機關，保留DPIA記錄並在適當時更新DPIA之義務仍然存在。

IV. Conclusions and recommendations
結論和建議

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

DPIA是資料控管者實施符合GDPR之資料運用系統的有效方式，且對某些類型之運用作業可能為強制性的。DPIA具有可延展性，可採用不同之形式，但GDPR對有效的DPIA設定了基本要求。資料控管者應將辦理DPIA視為有助於法律遵循的有效且積極之行動。

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*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項規定了控管者遵守GDPR之基本責任：「*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。必要時應檢視並更新*

這些措施」。

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.
當預計或正在實施高風險資料運用時，DPIA是遵守本規則之關鍵要素。此意味著資料控管者應使用本指引中規定之標準來確認是否須辦理DPIA。資料控管者內部政策可增列GDPR法律要求以外之標準於此清單中。如此可使當事人和其他資料控管者有更充足之信任和信心。

Where a likely high risk processing is planned, the data controller must:
當規劃可能造成高風險之運用時，資料控管者必須：

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:
  選擇符合附錄2標準之DPIA方法論（附錄1中提供之示例），或指定並執行符合以下要件之系統性之DPIA程序：
  - is compliant with the criteria in Annex2;
    符合附錄2中之標準；
  - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
    依據內部程序、環境和文化，整合至現有之設計、開發、變更、風險和營運審核程序中;
  - involves the appropriate interested parties and clearly define their responsibilities (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, *etc*.);
    納入適當利益關係人並明確界定其職責（控管者、DPO、當事人或其代理人、業務、技術服務、受託運用者、資訊安全長等）；
- provide the DPIA report to the competent supervisory authority when required to do so;
  於必要時向權責監管機關提供DPIA報告；
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;

在無法決定足以減輕高風險之措施時，諮詢監管機關；

- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
  定期檢視DPIA及其評估之運用，至少在運用作業所造成之風險發生變化時；
- document the decisions taken.
  記錄所採取之決定。

Annex 1 – Examples of existing EU DPIA frameworks
附錄1 –現行歐盟DPIA架構示例

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

GDPR並未明定必須遵循之DPIA程序，而是允許資料控管者在考量第35條第7項所描述之組成要素下，導入一個可補足其現行作業活動之架構。此架構可以是資料控管者所制定的，或是特定行業之共同架構。由歐盟DPA和歐盟特定部門先前所發展並公布之架構，包括（但不限於）：

Examples of EU generic frameworks:

歐盟通用架構示例：

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  德國：標準資料保護模型，V.1.0 - 試用版本，2016[31]。
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para unaEvaluación de Impactoen la Protección de DatosPersonales (EIPD)*, Agenciaespañola de protección de datos (AGPD), 2014.
  西班牙：*個人個資保護影響評估指南（EIPD）*，西班牙資料保護機關（AGPD），2014。
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  法國：*隱私影響評估（PIA）*，國家資訊及自由委員會（CNIL），2015。
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information

[31] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.
2016年11月9日至10日，聯邦和各州在Kühlungsborn （屈隆斯博恩）的獨立資料保護機關會議，92票一致且無異議通過（巴伐利亞邦棄權）。

Commissioner's Office (ICO),2014.

英國：*執行隱私影響評估實踐準則*，資訊主委辦公室（ICO），2014。

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:

歐盟特定部門架構示例：

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[32].

  RFID應用之隱私和個資保護影響評估架構[32]。

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[33]

  智慧電網和智慧計量系統之個資保護影響評估範本[33]。

  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[34]).

國際標準亦可為辦理DPIA之方法論提供指引（ISO/IEC 29134[34]）。

---

[32]See also :

請另參閱：

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification.
  2009年5月12日執委會關於以無線射頻辨識應用於執行隱私和資料保護原則之建議。
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.
  9/2011意見，關於RFID應用之隱私和個資保護影響評估架構之產業提案修正版。
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33]See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

請另參閱07/2013意見，關於由執委會智慧電網工作特別小組專家第2組編寫關於智慧電網和智慧計量系統之個資保護影響評估範本（「DPIA範本」）。

[34] ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

ISO/IEC 29134（計畫），*資訊科技 - 安全技術 - 隱私影響評估 – 指引*，國際標準化組織（ISO）。

Annex 2 – Criteria for an acceptable DPIA

附錄2 – 可接受之DPIA標準

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

WP29就資料控管者可用以評估所辦理之DPIA，或辦理DPIA之方法論，是否足以全面符合GDPR，提出了以下標準：

- ☐ a systematic description of the processing is provided (Article35(7)(a)):
  提供對運用作業系統性之描述（第35條第7項第a款）：
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
    運用之性質、範圍、背景和目的已納入考量（前言第90點）；
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
    已記錄之個人資料、接收者和個人資料儲存期限；
  - ☐ a functional description of the processing operation is provided;
    已提供運用作業之功能性描述；
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
    已確認個人資料所依賴之資源（硬體、軟體、網路、人員、文件或文件傳輸管道）；
  - ☐ compliance with approved codes of conduct is taken into account (Article35(8));
    已遵循經核准之行為守則（第35條第8項）；
- ☐ necessity and proportionality are assessed (Article35(7)(b)):
  已評估必要性及合比例性（第35條第7項第b款）：
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    確認為遵守本規則而預計採行之措施（第35條第7項第d款和前言第90點），同時考量到：
    - ☐ measures contributing to the proportionality and the necessity of the

processing on the basis of:

如下有助於使運用符合比例性和必要性之措施：

- ☐ specified, explicit and legitimate purpose(s) (Article5(1)(b));
  特定、明確及合法之目的（第5條第1項第b款）；
- ☐ lawfulness of processing (Article6);
  運用之合法性（第6條）；
- ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  適當、相關且限於必要之資料（第5條第1項第c款）；
- ☐ limited storage duration (Article5(1)(e));
  有限之儲存期限（第5條第1項第e款）；

☐ measures contributing to the rights of the data subjects:

有助於當事人權利之措施：

- ☐ information provided to the data subject (Articles 12, 13 and14);
  提供予當事人之資訊（第12、13和14條）；
- ☐ right of access and to data portability (Articles 15 and20);
  近用及資料可攜權（第15條和第20條）；
- ☐ right to rectification and to erasure (Articles 16, 17 and19);
  更正和刪除權（第16、17和19條）；
- ☐ right to object and to restriction of processing (Article 18, 19 and21);
  拒絕和限制運用權（第18、19和21條）；
- ☐ relationships with processors (Article 28);
  與受託運用者之關係（第28條）；
- ☐ safeguards surrounding international transfer(s) (Chapter V);
  國際傳輸之安全維護措施（第五章）；
- ☐ prior consultation (Article36).
  事前諮詢（第36條）。

☐ risks to the rights and freedoms of data subjects are managed (Article35(7)(c)):

已管理當事人權利和自由之風險（第35條第7項第c款）：

- ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  鑑別風險來源、本質、特殊性與嚴重性（請參閱前言第84點），或更具體來說，從當事人之觀點來看待每項風險（非法存取、未預期之修改和資料滅失）：
  - ☐ risks sources are taken into account (recital90);
    已考量風險來源（前言第90點）；
  - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    已確認當發生包含非法存取、未預期之修改和資料滅失等事件時，對當事人權利和自由之潛在影響；
  - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    已確認可能導致非法存取、未預期之修改和資料滅失之威脅；
  - ☐ likelihood and severity are estimated (recital90);
    已評估可能性和嚴重性（前言第90點）；
- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
  已決定預計用以因應這些風險之措施（第35條第7項第d款和前言第90點）；

☐ interested parties are involved:
利益關係人已參與：

- ☐ the advice of the DPO is sought (Article35(2));
  已尋求DPO之建議（第35條第2項）；
- ☐ the views of data subjects or their representatives are sought, where appropriate (Article35(9)).
  已酌情徵詢當事人或其代理人之意見（第35條第9項）。