ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

關於第2016/679號規則(GDPR)中的個人資料侵害通知之指引

Adopted on 3 October 2017

2017年10月3日通過

As last Revised and Adopted on 6 February 2018

2018年2月6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 Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 02/013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 CONTENTS 目錄

INTRODUCTION 導言

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

一般資料保護規則（GDPR）要求將個人資料之侵害（此後簡稱為「侵害」）通知國家監管機關[1]（或在跨境侵害之情況下，通知主責機關），並在某些情況下，須向個人資料因侵害而受影響之當事人就侵害進行溝通。

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

[1] See Article 4(21) of the GDPR
請參閱 GDPR 第 4 條第 21 款。

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 和 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611。

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
請參閱 https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm。

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046。

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
此為歐盟基本權利憲章所載之權利，請參閱http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT。

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

某些組織目前已存在侵害通知義務，例如公眾電子通信服務提供者（如2009/136/EC指令和第611/2013號規則（EU）中所規定）[2]。也有部分歐盟成員國已有其國內的侵害通知義務，這可能包括某些類別之控管者和公眾電子通信服務提供者的侵害通知義務（例如德國和義大利），或有義務通報所有個人資料侵害案件（例如荷蘭）。其他成員國可能有相關之業務守則（例如愛爾蘭[3]）。雖然許多歐盟資料保護機關目前皆鼓勵控管者通報侵害行為，但被GDPR取代的95/46/EC個人資料保護指令[4]並未包含具體的侵害通知義務，因此對許多組織而言，這將會是一項新的要求。GDPR現在強制要求所有控管者應負通知義務，除非該侵害不太可能對個人的權利和自由造成風險[5]。受託運用者也扮演重要的角色，任何侵害發生必須通知控管者[6]。

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

29條工作小組（WP29）認為此項新的通知要求有許多益處。在通知監管機關時，控管者可就是否需通知受影響之個人獲得建議。當然監管機關可能要求控管者將侵害事件通知該個人[7]。透過與個人溝通侵害事件，控管者可以提供因該侵害所帶來的風險之資訊，以及個人為保護自身免受潛在後果影響得採取之保護措施。任何侵害應變計劃之重點應該著重於保護當事人及其個人資料。因此，侵害通知應被視為係強化關於遵循個人資料保護之工具。同時應注意，漏未向個人或監管機關通知侵害之發生可能意味著第83條之罰鍰可能適用於控管者。

Controllers and processors are therefore encouraged to plan in advance and put in place processes

請參閱第 33 條第 2 項。此與（EU）第 611/2013 號規則第 5 條的概念類似，該條款規定，若發生個人資料侵害事件，以契約約定提供部分電子通信服務的提供者（與用戶沒有直接的契約關係）有義務通知契約提供者該侵害。

[7] See Articles 34(4) and 58(2)(e)
請參閱第 34 條第 4 項和第 58 條第 2 項第 e 款。

to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.
因此鼓勵控管者和受託運用者提前計劃並實施相關步驟，以便能夠檢測並迅速控制侵害，進而評估對個人造成之風險[8]，然後確認是否有必要通知監管機關，並在必要時就侵害與相關個人進行溝通。通知監管機關應屬於事故應變計畫之一部分。

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.
GDPR規定了何時需要通知侵害、通知之對象以及通知應包含何種資訊。該通知應包含之資訊可分階段提供，但在任何情形下，控管者皆應及時對任何侵害採取行動。

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.
在關於個人資料侵害通知之03/2014意見中[9]，WP29提供指導以協助控管者判斷在發生侵害時是否應通知當事人。該意見考量了2002/58/EC指令有關電子通信服務提供者之義務，並提供了多個產業的示例，然後以此脈絡草擬GDPR，並為所有控管者提供優良實務範例。

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.
本指引說明了GDPR的強制侵害通知義務和溝通要求，以及控管者和受託運用者為符合其新義務可採取的一些步驟。本文件亦舉例說明了各種類型之侵害以及在不同可能情境下需要

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).
這可以在 DPIA 的監測和審查要求下得到確保，DPIA(個資保護影響評估)對於可能導致自然人權利和自由的高風險的處理操作是必要的（第 35 條第 1 項和第 11 項）。

[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
請參閱關於個人資料侵害通知之 03/2014 意見 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf。

被通知之對象。

I. Personal data breach notification under the GDPR
GDPR之個人資料侵害通知

A. Basic security considerations
基本安全考量因素

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].

GDPR的要求之一，係透過採用適當技術性與組織性措施，個人資料應可以確保適當安全性之方法運用，包括防止未經授權或非法運用以及防止意外遺失、破壞或毀損[10]。

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].

因此，GDPR要求控管者和受託運用者皆須採取適當之技術性與組織性措施，以確保安全層級與運用個人資料產生之風險相當。相關措施應考量到現有技術水準、執行成本和資料運用之性質、範圍、背景及運用目的，以及對自然人權利和自由之風險變動的可能性和嚴重性[11]。此外，不論是否已有侵害發生，GDPR亦要求立即建置所有的適當技術性保護組織措施，以確認該措施是否已包含通知義務[12]。

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

因此，任何資料安全政策的關鍵要素是，能夠在可能的情況下，防止侵害之發生，並於仍

[10] See Articles 5(1)(f) and 32.
請參閱第 5 條第 1 項第 f 款以及第 32 條。

[11] Article 32; see also Recital 83
第 32 條；另請參閱前言第 83 點。

[12] See Recital 87
請參閱前言第 87 點。

發生侵害情事時，及時對其作出反應。

B. What is a personal data breach？

何謂個人資料侵害?

1. Definition

定義

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a “personal data breach” in Article 4(12) as：

因應侵害的第一步是控管者須先能識別該侵害。GDPR第4條第12款將「個人資料侵害」定義為：

> “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
>
> 「違反安全性導致傳輸、儲存或以其他方式運用之個人資料遭意外或非法破壞、遺失、變更、未經授權揭露或存取使用。」

What is meant by “destruction” of personal data should be quite clear： this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. “Damage” should also be relatively clear： this is where personal data has been altered, corrupted, or is no longer complete. In terms of “loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

「破壞」個人資料之定義應已非常明確：係指資料不存在，或不再以對控管者有用之形式存在。「毀損」之定義也應相對明確：係指個人資料已被更改、損毀或不再完整。就個人資料「遺失」而言，應可被解釋為資料可能仍然存在，但控管者失去對該資料之控制或存取，或不再擁有該資料。最後，未經授權或非法運用可能包括向未被授權接收（或存取）資料之接收者揭露（或使其存取）個人資料，或違反GDPR規範之其他任何形式之運用。

Example

示例

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

個人資料遺失之示例可包括控管者客戶資料庫副本儲存設備遺失或遭竊。遺失的另一個例子可能是個人資料集的唯一副本已被勒索軟體加密，或者已被控管者加密卻不再擁有加密金鑰。

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].

侵害屬於一種安全事故應已十分明確。然而，如第4條第12款所示，GDPR僅適用於侵害*個人資料*之情事。侵害發生之後果在於控管者將無法確保遵守GDPR第5條所規範之個人資料運用相關原則。這突顯了安全事故和個人資料侵害之間的區別 – 本質上，雖然所有個人資料侵害皆屬於安全事故，但並非所有的安全事故都必然是個人資料之侵害[13]。

The potential adverse effects of a breach on individuals are considered below.

侵害對個人的潛在不利影響說明如下。

2. Types of personal data breaches

個人資料侵害類型

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]：

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.
應該注意的是，安全事件不僅限於從外部來源對組織進行攻擊之威脅型態，而亦包括因內部運用違反安全原則之事件。

[14] See Opinion 03/2014
請參閱 03/2014 意見。

WP29在03/2014關於侵害通知之意見中說明，「侵害」可依據以下三項著名的資訊安全原則進行分類[14]：

- “Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.
  「機密性之侵害」- 未經授權或意外揭露或存取個人資料之情形。

- “Integrity breach” - where there is an unauthorised or accidental alteration of personal data.
  「完整性之侵害」- 未經授權或意外變更個人資料之情形。

- “Availability breach” - where there is an accidental or unauthorised loss of access[15]to, or destruction of, personal data.
  「可用性之侵害」- 意外或未經授權遺失存取[15]或破壞個人資料之情形。

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.
亦需注意，依情況，侵害可能同時涉及個人資料之機密性、完整性和可用性，及其任何組合。

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.
是否存在機密性或完整性侵害相對而言較為明確，而是否存在可用性侵害則較不明顯。當個人資料永久遺失或破壞時，皆會被認為是可用性侵害。

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines “availability” as: "Ensuring timely and reliable access to and use of information," available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: " Timely, reliable access to data and information services for authorized users." See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines “availability” as “Property of being accessible and usable upon demand by an authorized entity”: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en
一般公認「存取」基本上屬於「可用性」之一環。 例如，請參閱NIST SP800- 53rev4將「可用性」定義為：「確保得及時且確實存取和使用資訊」。請查詢 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf。CNSSI-4009亦提及：「為授權用戶提供及時且確實存取資料和資訊服務。」請參閱https://rmf.org/wp- content/uploads/2017/10/CNSSI-4009.pdf. 。ISO/IEC 27000：2016亦將「可用性」定義為「依據授權實體之要求可存取和使用之資產」：https://www.iso.org/obp/ui/#iso:std:iso- iec:27000:ed-4:v1:en。

Example

示例

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

遺失可用性之示例包括資料被意外或未經授權之人刪除，或遺失安全加密資料的解密金鑰。若控管者無法恢復對資料之存取，例如，從備份中恢復，則這將被視為永久遺失可用性。

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

若組織的正常服務受到嚴重干擾，也可能會造成可用性遺失，例如，遇到電源故障或阻斷服務攻擊，導致無法使用個人資料。

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, “security of processing,” explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to “the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,” and “the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”.

可能會被提出的問題是，暫時喪失個人資料可用性是否應被視為可用性之侵害，若是，則需通知。GDPR第32條「運用之安全」說明，在實施技術性與組織性措施以確保安全層級與風險相當時，除其他要件外，「可持續確保運用系統和服務之機密性、完整性、可用性和彈性的能力」，與「在實體環境或技術性事故中，能及時恢復個人資料的可用性和存取的能力」亦應納入考量。

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a ‘breach of security’ as defined in Article 4(12).

因此，導致個人資料在一段時間內無法使用的安全事故也屬於一種侵害，因為無法存取資料會對自然人之權利和自由產生重大影響。明確地說，因執行計畫性之系統維護而無法存取個人資料不屬於第4條第12款所定義之「安全性之侵害」。

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals’ rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

與個人資料之永久遺失或破壞（或實際上任何其他類型之侵害）相同，涉及暫時喪失可用性之侵害應依據第33條第5項予以記錄。這有助於控管者向監管機關證明其責任，監管機關可能會要求查看該紀錄[16]。然而，依據侵害情況，可能需要通知監管機關及與受影響之個人溝通，也可能不需要。控管者將需評估因缺乏個人資料之可用性，對自然人權利和自由影響的可能性和嚴重性。依據第33條，除非該侵害不太可能對個人之權利和自由造成風險，否則控管者將需要通知。當然，這將需要依據個案進行評估。

[16] See Article 33(5)
請參閱第 33 條第 5 項。

Examples

示例

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

在醫院中，若無法使用關於病患的關鍵醫療資料，即使是暫時的，亦會對個人之權利和自由帶來風險；例如，手術可能被取消並將患者生命置於危險之中。

Conversely, in the case of a media company's systems being unavailable for several hours (e.g.due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

反之，在數小時無法使用媒體公司系統的情況下（例如因為停電），若該公司因此無法向其用戶發送定期通訊，則不太可能對個人的權利和自由構成風險。

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

應注意的是，儘管控管者的系統可能只是暫時喪失可用性，且可能不會對個人產生影響，但重要的是，控管者仍必須考量該侵害所有可能造成的後果，因為控管者可能因其他原因仍負通知義務。

Example

示例

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

若可從備份中恢復資料，感染勒索軟體（惡意軟體加密控管者之資料直到支付贖金）可能會導致暫時失去資料的可用性。然而，網路入侵已發生，若該事故符合機密性之侵害（例如個人資料遭攻擊者存取之情形），對個人的權利和自由造成風險，則可能需要通知。

3. The possible consequences of a personal data breach
個人資料侵害之可能後果

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[17].

侵害可能會對個人產生一系列潛在的重大不利影響，從而導致人身、財物或非財物的損害。GDPR說明這可能包括失去對個人資料之控制、對其權利之限制、歧視、冒用身分或詐欺、財務損失、未經授權之假名化還原、名譽損害以及受專業秘密保護之個人資料機密性之喪失。此亦包括其他任何對個人經濟的或社會的重大不利益之情形[17]。

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].

因此，GDPR要求控管者將侵害通知權責監管機關，除非不太可能導致此類不利影響之風險發生。若發生此類不利影響之風險甚高，則GDPR要求控管者在合理可行的情況下儘速與受影響之個人就該侵害進行溝通[18]。

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR：

GDPR前言第87點強調能夠識別侵害、評估其對個人之風險以及在必要時通知之重要性：

[17] See also Recitals 85 and 75.
請參閱前言第 85 點及第 75 點。

[18] See also Recital 86.
請參閱前言第 86 點。

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."
「應查明是否已實行所有適當之技術性保護與組織性措施，以便立即確認個人資料侵害是否發生，並快速通知監管機關和當事人。通知並未無故遲延之事實，尤應考量個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響。該通知可能導致監管機關依據本規則所訂定之任務或權力進行干預。」

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.
對個人不利影響之風險評估相關指引請參見第IV節。

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state： "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889
詳細資訊請參閱29條工作小組關於適用與訂定行政罰鍰之指引，請查閱：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889。

(Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

若控管者漏未通知監管機關與受侵害之當事人或其中一方，即使已符合第33條和/或第34條之要求，監管機關得依據第58條第2項之規定或其自身之決定，就所有可行之矯正措施做出選擇，包括考量處以適當之行政罰鍰[19]。若其選擇行政罰鍰，依據GDPR第83條第4項第a款，可處以最高10,000,000歐元或企業前一年度全球年營業額2%之罰鍰。亦須注意的是，在某些情況下，漏未進行侵害通知可能顯示現有安全措施之缺乏或現有安全措施之不足。WP29關於行政罰鍰之指引敘明：「在任何特定單一案件中，同時發生若干不同之侵害行為，意味著監管機關能夠在最嚴重侵害之範圍內，對其處以有效、符合比例和具有勸阻性程度之行政罰鍰」。在此情形下，監管機關亦可能一方面就漏未通知或溝通侵害事故（第33條和第34條）處罰，另一方面就缺乏（適當的）安全措施（第32條）予以處罰，因其屬兩種單獨的侵害行為。

II. Article 33 - Notification to the supervisory authority
第33條 - 通知監管機關

A. When to notify
何時通知

1. Article 33 requirements
第33條之要求

Article 33(1) provides that：

第33條第1項規定：

> “In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”
>
> 「於個人資料侵害發生時，控管者即應依第55條通報權責監管機關，不得無故遲延，且如可能，應於知悉後72小時內通報，但個人資料侵害不致對當事人權利和自由造成風險時，不在此限。如未能於72小時內通報監管機關，通報時應併附遲延之理由。」

Recital 87 states[20]：
前言第87點指出[20]：

> “It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.”
> 「應查明是否已實行所有適當之技術性保護與組織性措施，以立即確認個人資料侵害是否發生，並快速通知監管機關與當事人。判斷該通知非無故遲延之事實，尤應考量對個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響。該通知可能導致監管機關依據本規則所訂定之任務或權力進行干預。」

2. When does a controller become “aware”?
控管者「知悉」之時點為何？

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become “aware” of a breach. WP29 considers that a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
如上所述，GDPR要求，在侵害發生時，控管者應在沒有不當遲延的情況下通知侵害行為，且如可能，應於知悉後72小時內為之。此處的問題是何時得認定控管者已「知悉」侵害之發生。WP29認為，當控管者就發生危及個人資料的安全事故已具有合理程度的確定時，該控管者應可被認定為已「知悉」。

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into

[20] Recital 85 is also important here.
前言第 85 點於此處亦同等重要。

account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.
然而，如前所述，GDPR要求控管者實施所有適當之技術性保護與組織性措施，以立即確認是否有侵害發生，並及時通知監管機關和當事人。此外，判斷該通知非無故遲延之事實，尤應考量對個人資料侵害之本質與嚴重性及其對當事人產生之後果與不利影響[21]。這使控管者有義務確保及時「知悉」任何侵害情事，以便採取適當的行動。

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.
要確切認定何時控管者得被視為「知悉」特定之侵害，將取決於具體侵害之情況。在某些情況下，侵害從一開始就相對明顯，而於其他情況，則需要時間判斷是否已危及個人資料。然而，重點應在於迅速採取行動調查事故，以確認個人資料是否確實遭到侵害，如果是，則採取補救措施並在必要時通知。

[21] See Recital 87
請參見前言第 87 點。

Examples

示例

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become “aware” when it realised the USB key had been lost.

在遺失存有未加密個人資料的USB 智能儲存裝置*的情況下，通常不可能確認未授權之人是否已存取該資料。然而，即使控管者可能無法確認是否發生機密性侵害，但由於發生侵害之可能性已具有合理程度的確定性，因此必須通知。當控管者瞭解到USB智能儲存裝置遺失時，可被視為「知悉」。

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become “aware”.

第三方通知控管者，他們意外取得其一位客戶的個人資料，並提供該項資料係未經授權揭露之證據。由於控管者已經獲得機密性侵害的明確證據，因此毫無疑問地，控管者可被視為「知悉」。

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become “aware”.

控管者偵測到其網路可能遭受入侵。經控管者檢查其系統並確認該系統所保存之個人資料已受危害。由於控管者現已有侵害的明確證據，因此毫無疑問地可被視為「知悉」。

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

一名網路罪犯於駭入控管者之系統後與其聯繫以勒索贖金。於此情形下，在檢查其系統並確認已遭到攻擊後，控管者已有發生侵害的明確證據，因此毫無疑問可被視為「知悉」。

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short

*註釋：USB Key是一種智能儲存裝置，有CPU晶片可進行加解密運算，通常用於身分認證，與一般USB隨身碟不同。

period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being “aware”. However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

控管者於首次經由個人、媒體組織或其他來源告知可能發生侵害，或自行偵測到安全事故時，可進行短期調查，以確認侵害是否確實發生。在此調查期間，控管者得不被視為已「知悉」。然而，應盡快展開初步調查，並以合理程度的確信來判斷是否發生侵害；之後再進行更詳細之調查。

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

一旦控管者已知悉，屬應通知之侵害應立即通報，不得無故遲延，且如果可能，該通報不得晚於72小時。在此期間，控管者應評估個人可能面臨之風險，以決定是否已觸發通報要求，以及處理侵害所需之行動。然而，控管者或許已對侵害可能導致之潛在風險進行初步評估，該初步評估可能來自於執行相關運用操作前所進行的個資保護影響評估（DPIA）[22]其中一部分。然而，與任何實際侵害的特定情狀相比，DPIA(評估的情況)可能較為一般，因此無論如何，都需在考量上開特定情狀下進行額外之評估。有關風險評估的進一步資訊，請參閱第IV節。

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

在大多數情況下，於初次預警後，隨後應完成這些初步行動 (即當控管者或受託處理者懷疑發生可能涉及個人資料之安全事故時) – 僅在例外情況下始得允許較長的時間。

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
請參閱 29 條工作小組關於 DPIAs 指引，請查閱 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。

Example
示例

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

當事人通知控管者收到冒充控管者的電子郵件，其中包含與該當事人（實際）使用控管者服務相關之個人資料，意味著控管者的安全性已遭受危害。控管者進行短期調查並確認其網路遭入侵以及未經授權存取個人資料之證據。控管者於此時將被視為「知悉」，並且需通報監管機關，除非該侵害不太可能對個人的權利和自由構成風險。控管者將需採取適當的補救措施來解決該侵害。

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

因此，控管者應有內部流程，以便能夠偵測並處理侵害之發生。例如，為發現非常規之資料運用行為，控管者或受託運用者得使用某些技術性措施，例如資料流和(電腦)日誌分析器，從中藉由任何日誌資料之關聯得以辨識出事件和預警[23]。重要的是，當偵測到侵害時，須向上通報至適當的管理階層，以便於處理，並於符合第33條要件時依該條進行通報、必要時

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.
應當注意，促進例如資料的儲存、修改或刪除的可審計性之日誌資料亦可被認為係與開始相應運用操作之人的相關個人資料。

並依據第34條進行通知。此類措施和通報機制可在控管者的事故應變計畫和/或公司治理規劃中詳細描述。這將有助於控管者有效規劃並確認組織內負責管理侵害之人員以及如何或是否酌情升高事故等級。

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).
控管者亦應與其所使用之任何受託運用者採取適當安排，當發生侵害時，受託運用者有義務通知控管者（請參閱下文）。

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.
控管者和受託運用者有責任採取適當之措施來防止、因應與處理侵害，對此，有一些應適用於所有案件的實際步驟

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
  所有與安全事件相關之資訊應直接交付予負責人員，或其任務為處理事故、確認侵害之存在以及評估風險之人員。

- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
  然後應評估因侵害而導致之個人風險（無風險、風險或高風險之可能性），並通知組織的相關部門。

- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
  必要時，應通報監管機關，並與受影響之當事人就侵害進行可能的溝通。

- At the same time, the controller should act to contain and recover the breach.
  同時，控管者應採取行動以控制和挽救該侵害。

- Documentation of the breach should take place as it develops.
  應全程記錄侵害事故之發展。

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

因此，很清楚的是，控管者有義務對任何初次預警採取行動，並確認侵害是否實際發生。允許在短暫的期間內進行一些調查，並讓控管者蒐集證據和其他相關詳情。然而，一旦控管者對侵害之發生具有合理程度之確定時，如符合第33條第1項之要件，則應通報監管機關，不得無故遲延，且如果可能，不得晚於72小時[24]。若控管者未能及時採取行動並且顯然確實發生了侵害，則控管者可能被視為未依據第33條進行通報。

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data： the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

第32條明確規範控管者和受託運用者應採取適當技術性與組織性措施，以確保個人資料的適當安全等級：得以及時偵測、處理和報告侵害之能力，應被視為這些措施之基本要素。

3. Joint controllers

共同控管者

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

第26條規範共同控管者，並規定共同控管者應確定為履行GDPR其各自應負之責任[25]。這將包括確定哪一方有依第33條和第34條規定遵守相關義務之責。WP29建議共同控管者間之契約安排應包括確認哪一方控管者將主導或負責遵守GDPR侵害通知義務之規定。

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN
請參閱第 1182/71 號規則關於確認適用於期間、日期和時間限制之規則，請查閱：http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN。

[25] See also Recital 79.
請參閱前言第 79 點。

4. Processor obligations

受託運用者之義務

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor “assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor”.

控管者就個人資料的保護負有全面性之責任，但受託運用者在協助控管者遵守其義務上扮演重要角色；這包括侵害之通知。實際上，第28條第3項明定受託運用者所為之處理應受契約或其他立法之拘束。第28條第3項第f款指出，契約或其他立法應規定受託運用者「考量運用之性質和受託運用者可得之資訊，協助控管者確保遵守第32至第36條所訂之義務」。

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller “without undue delay”. It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as “aware” once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

第33條第2項明確規定，若控管者利用某受託運用者，且該受託運用者知悉其代表控管者運用之個人資料遭到侵害，則應通知控管者，且「不得無故延遲」。應注意，受託運用者在通知控管者之前不需先行評估因侵害而引起風險的可能性，此為控管者在知悉侵害時所必須進行之評估。受託運用者只需確認是否有侵害之發生並通知控管者。控管者係利用受託運用者來實現其特定目的，因此，原則上一旦受託運用者已向其通知該項侵害，控管者應

被視為「知悉」。受託運用者通知控管者之義務使得控管者得解決侵害，並確認是否需要依據第33條第1項通報監管機關和依據第34條第1項通知受影響之當事人。因受託運用者或許無法獲知所有與該事件相關的事實，所以控管者可能也希望調查該侵害，例如，若控管者仍保留了被受託運用者毀損或遺失的個人資料副本或備份。這可能會影響控管者是否因而需要通知。

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore, WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.
GDPR就受託運用者必須於何時限內向控管者提出警示並無明確規定，僅規定「不得無故遲延」。因此，WP29建議受託運用者迅速通知控管者，當獲得更多細節時，可分階段提供有關侵害之進一步資訊。這對於幫助控管者滿足在72小時內向監管機關通知之義務相當重要。

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller’s obligations to report to the supervisory authority within 72 hours.
如上所述，控管者和受託運用者間之契約除了需包含GDPR中之其他規範外，應闡明如何滿足第33條第2項所述之要求。這可包括要求受託運用者儘早通知，以協助控管者符合在72小時內向監管機關通報之義務。

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.
若受託運用者提供服務的多個控管者皆受同一事故影響，則受託運用者必須對每個控管者通報該事故的詳細資訊。

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.
若控管者已給予受託運用者適當之授權，且該授權係控管者和受託運用者間契約安排的一部分，則受託運用者可代表控管者進行通知。該通知必須符合第33條和第34條之規定。然而，須特別注意通知的法律責任仍由控管者承擔。

B. Providing information to the supervisory authority
向監管機關提供資訊

1. Information to be provided
所須提供之資訊

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should：

當控管者向監管機關通報侵害時，第33條第3項規定，該通報至少應：

> "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> 「描述個人資料侵害之性質，如有可能，應包括相關當事人之類別和大致數量，以及相關個人資料紀錄之類別和大致數量；
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> 告知個資保護長之姓名和聯繫方式，或其他可獲取更多資訊之聯絡點；
>
> (c) describe the likely consequences of the personal data breach;
>
> 描述個人資料侵害之可能結果
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."
>
> 描述控管者為解決個人資料侵害而採行或預計採行之措施，在適當情況下，包括降低可能不利影響之措施。」

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach： depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

GDPR就當事人或個人資料紀錄之類別並無定義。然而，WP29建議當事人之類別係指個人

資料受侵害影響之各類人員：依據所使用之描述，這可能包括兒童及其他弱勢群體、殘疾人士、員工或客戶等。同樣地，個人資料紀錄的類別可指控管者所運用的不同類型之紀錄，例如健康資料、教育紀錄、社會照護資訊、財務細節、銀行帳號，護照號碼等。

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

前言第85點明確指出，通知的目的之一係限縮對個人造成之損害。因此，若當事人之類型或個人資料之類型顯示因侵害而發生特定損害之風險（例如冒用身分、詐欺、財務損失、對職業秘密之威脅），則於通知中表明這些類別是很重要的。透過此方式，可與描述該侵害可能後果之要求產生連結。

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

無法掌握準確之資訊（例如受影響當事人的確切數量）不應成為及時通報該侵害之阻礙。GDPR允許就受影響的個人數量和相關個人資料紀錄的數量粗略估計。重點應直接針對解決侵害的不利影響，而非提供準確的數字。

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

因此，若侵害之發生已十分明確，但侵害程度未明，則分階段通知（見下文）是履行通知義務的安全方式。

Article 33(3) states that the controller “shall at least” provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

第33條第3項規定，控管者「應至少」於通知中提供該等資訊，使控管者得於必要時選擇提供進一步的細節。不同類型之侵害（機密性、完整性或可用性）可能需要進一步的資訊以充分說明每個案件之情況。

Example

示例

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

若侵害發生之根本原因來自於受託運用者，特別是該事故係因同一受託運用者致使其他許多控管者的個人資料紀錄皆受到影響時，控管者於通報監管機關時，同時告知該受託運用者之名稱將對控管者有所助益。

In any event, the supervisory authority may request further details as part of its investigation into a breach.

無論如何，監管機關可能會要求進一步之細節作為其侵害調查的一部分。

2. Notification in phases

分階段通知

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states：

依據侵害之性質，控管者可能必須做進一步調查，以確認與事故相關之所有事實。因此，第33條第4項規定：

> "Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."
>
> 「在無法同時提供資訊的情形下，可分階段提供資訊，不得有進一步之無故遲延。」

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29

recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.
此意味著GDPR認識到控管者在知悉侵害後的72小時內並不一定可掌握有關侵害的所有必要資訊，因為在此初始階段可能無法取得完整而全面的事故詳情。因此，GDPR允許分階段通知。此情形在複雜的侵害事故中更有可能發生，例如發生某些類型的網路安全事故時，需要進行深入的司法鑑定調查，以充分確認侵害之性質以及個人資料遭損害之程度。於是在許多情況下，控管者必須進行更多調查，並繼續跟進以取得進一步資訊。因此第33條第1項允許控管者於延遲通報之情況下併附理由。WP29建議，若控管者於首次通報監管機關時尚未取得所有必要資訊，控管者應同時告知監管機關，將於日後提供更多詳細資訊。監管機關應決定該項詳細資訊應如何及何時提供。但若控管者一旦知悉必須提供給監管機關之與侵害相關的其他細節，該決定並不妨礙控管者在任何其他階段提供進一步的資訊。

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.
要求通報之目的係鼓勵控管者對侵害迅速採取行動、控制侵害並儘可能回復受損之個人資料，並向監管機關尋求相關建議。在最初的72小時內通報監管機關可協助控管者確認關於通知或不通知當事人之決定是否正確。

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to

[26] See Article 9.
請參閱第 9 條。

communicate the breach to the data subject where it is required.

然而，通報監管機關之目的不僅在於取得是否應通知受影響當事人之指導。在某些情況下，由於侵害之性質和風險的嚴重程度，控管者很明顯地必須立即通知受影響之當事人，不得遲延。例如，有冒用身分的立即威脅或特殊類別個人資料在線上被揭露[26]時，控管者應採取行動控制侵害並與受影響之當事人就該侵害進行溝通，不得無故遲延(請參閱第III節)。在特殊情況下，甚至可能在通報監管機關前即須採取行動。一般來說，對監管機關之通知不得作為未在需要時與當事人溝通該項侵害之正當理由。

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

亦應釐清的是，在進行首次通報後，若後續調查證據顯示安全事故已被控制且並無實際侵害發生，控管者可向監管機關更新資訊。這些資訊可增列至已提供給監管機關的資訊中，因此該項紀錄即不屬於侵害事故。通報最後並未造成侵害之事故不會導致罰鍰。

Example

示例

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

控管者在發現遺失包含某些客戶個人資料副本的USB智能儲存裝置的72小時內通報監管機關。而後發現係控管者內部歸檔錯誤，該USB智能儲存裝置失而復得。控管者向監管機關更新資訊並請求修正通報。

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

另應注意的是，2002/58/EC指令、第611/2013號規則和其他自行通報事故之現有義務，皆已採用分階段通報方式。

3. Delayed notifications
遲延通報

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

第33條第1項明確規定，若未於72小時內向監管機關通報，則通報應附遲延之理由。依據該規定與分階段通知之概念可知，已認知控管者可能無法皆於規定時間內通報侵害，因此遲延通報可被允許。

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

此種情況可能發生於，例如控管者在短時間內經歷多個相類似的機密性侵害，並同樣影響大量當事人。控管者可能已知悉侵害，同時開始調查，但在通報前，再偵測出不同起因的類似侵害。依據具體情況，控管者可能需要一段時間來確認侵害程度，與其單獨通報各項侵害，不如讓控管者將數個非常相似但起因各異之侵害整理為一份有意義的通報。這就可能導致該項對監管機關之通報遲延並超過控管者首次知悉侵害之72小時。

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a “bundled” notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

嚴格來說，個別侵害皆是可通報事故。然而，為了避免過度負擔，若涉及在相對短時間內以相同之方式侵害相同類型之個人資料，控管者可提交包含所有侵害之「包裹」通報。若涉及不同類型個人資料的一連串侵害，且以不同方式侵害，則必須依一般方式通報，即每

項侵害皆須依據第33條進行通報。

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.
雖然GDPR允許在一定程度上之遲延通報，但這不應被視為常態。另需指出，有數個類似侵害須於72小時內通報時，亦可適用包裹通報。

C. Cross-border breaches and breaches at non-EU establishments
跨境侵害以及發生在非設立於歐盟據點之侵害

1. Cross-border breaches
跨境侵害

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that：
在跨境運用[27]個人資料時，侵害可能會影響一個以上成員國之當事人。第33條第1項明確規定，當侵害發生時，控管者應依據GDPR第55條[28]通報權責監管機關。第55條第1項規定：

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."
> 「各監管機關應有權於其成員國領土內依本規則執行指定之職務並行使公權力。」

However, Article 56(1) states：
然而，第56條第1項規定：

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

[27] See Article 4(23).
請參閱第 4 條第 23 項。

[28] See also Recital 122.
請參閱前言第122點。

「在不妨礙第55條之前提下，控管者或受託運用者之主要據點或單一據點的監管機關，為了第60條規定之程序，應足擔任該控管者或受託運用者之跨境運用行為的主責監管機關。」

Furthermore, Article 56(6) states：

此外，第56條第6項規定：

“The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.”

「主責監管機關應為控管者或受託運用者執行跨境運用時之唯一溝通對口。」

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

此意味著在跨境運用中發生侵害，且須通報時，控管者將需通報主責監管機關[29]。因此，在草擬侵害應變計畫時，控管者應評估何監管機關是其所需通報的主責監管機關[30]。這將有助

[29] See WP29 Guidelines for identifying a controller or processor’s lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.
請參閱 WP29 關於辨別控管者或受託運用者之主責監管機關指引，請查閱：http://ec.europa.eu/newsroom/document.cfm?doc_id=44102。

[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm
所有歐洲國家資料保護機關之聯繫方式列表請查閱：
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

於控管者迅速對侵害做出回應，以履行其依第33條規定之義務。因此，若侵害事件涉及跨境運用，必須通報主責監管機關，該機關之所在地不必是受影響當事人的所在地，或侵害發生地。在通知主責機關時，控管者於適當情況下應說明侵害是否涉及位於其他成員國之據點，以及何成員國內之當事人可能受到該侵害之影響。若控管者對主責監管機關之認定有疑義時，該控管者應至少通知侵害發生地之監管機關。

2. Breaches at non-EU establishments

發生在非設立於歐盟境內機構之侵害

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]：

第3條規範之GDPR地域範圍，包括當其適用於非設立於歐盟境內的控管者或受託運用者所為之個人資料運用的情況。特別是，第3條第2項規定[31]：

> "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> 「本規則適用於非設立於歐盟境內之控管者或受託運用者對位於歐盟境內之當事人所為涉及如下事項之個人資料運用：
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> 對歐盟境內之當事人提供商品或服務，不問是否需要當事人付款;或
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."
>
> 監控當事人於歐盟境內之行為」

Article 3(3) is also relevant and states[32]：

第3條第3項亦與此相關並規定[32]：

[31] See also Recitals 23 and 24
請另參閱前言第 23 點及第 24 點。

[32] See also Recital 25.
請另參閱前言第 25 點。

> “This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.”
> 「本規則適用於設立在非歐盟境內，但依國際公法而適用成員國法律之領域的控管者所為之個人資料運用。」

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller’s representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).

因此，當非設立於歐盟境內之控管者符合第3條第2項或第3條第3項要件且有侵害之發生時，仍受第33條和第34條通報義務之拘束。第27條規定當控管者（和受託運用者）有第3條第2項情形時應指定在歐盟境內之代表。在此情形下，WP29建議應通報控管者指定之歐盟境內代表所在成員國之監管機關[33]。同樣，若受託運用者符合第3條第2項要件時，其亦受受託運用者之義務拘束，而與此處特別相關者，即為依據第33條第2項通知控管者侵害之義務。

D. Conditions where notification is not required
無需通報之情形

Article 33(1) makes it clear that breaches that are “unlikely to result in a risk to the rights and freedoms of natural persons” do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

第33條第1項明確規定，「不太可能對自然人權利和自由造成風險」之侵害無需通報監管機關。例如可能是個人資料已經公開可用，且該資料之揭露不會對個人構成可能之風險。此一規定與現行2009/136/EC指令中公眾使用電子通信服務提供者之侵害通報要求不同，該指

[33] See Recital 80 and Article 27.
請參閱前言第 80 點和第 27 條。

令規定所有相關侵害皆須通知權責機關。

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.
在有關侵害通報的03/2014意見中[34]，WP29說明，以最先進演算法加密之個人資料遭受機密性侵害，仍屬個人資料之侵害，因此必須通報。然而，若金鑰之機密性是完整的 – 即金鑰在任何安全侵害中皆未受損，且其產生方式讓任何未經授權存取之人無法透過可用之技術查出 – 則基本上資料是無法解讀的。因此，侵害不太可能對個人產生不利影響，因此亦無需與當事人進行溝通[35]。然而，即使資料被加密，若控管者沒有適當的備份，該資料遺失或變更亦會對當事人產生負面影響。在此情形下，即使資料本身有適當的加密措施，也需要與當事人進行溝通。

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.
WP29亦說明，若個人資料（如密碼）經雜湊與亂數（salted）安全地處理，即雜湊值(Hash值)是以最先進的加密金鑰雜湊函數計算，那麼用於雜湊資料之金鑰將不會在任何侵害中受到損害。且用於雜湊資料之金鑰的產生方式讓任何未經授權存取之人無法透過可用之技術查出。

Consequently, if personal data have been made essentially unintelligible to unauthorised parties

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
WP29，有關侵害通知03/2014意見，請查閱http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf。

[35] See also Article 4(1) and (2) of Regulation 611/2013.
請另參閱611/2013規則第4條第1和2款。

and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

因此，若個人資料對於未授權方而言基本上無法解讀，且資料之副本或備份亦存在，則涉及適當加密之個人資料機密性侵害可能不太需要向監管機關通報。這是因為此種侵害不太可能對個人之權利和自由構成風險，而無高風險之可能也意味著不需要通知當事人。然而，仍須記住，雖然最初可能因為對個人的權利和自由並無可能之風險而無須通報，但這或許會隨著時間的推移而發生變化，並必須重新評估風險。例如，若隨後發現金鑰遭到損害，或加密軟體的漏洞被揭露，則可能仍然需要通報。

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

此外，應需注意，若侵害發生在加密卻沒有備份之個人資料，則可能存在可用性侵害，而對個人構成風險，因此也許需要通知。同樣，若侵害之發生涉及加密資料的遺失，即使存在個人資料備份，仍可能構成可通報之侵害，具體判定取決於從該備份回復資料所需的時間長短，以及欠缺可用性時對個人之影響。如第32條第1項第c款所述，安全的一個重要因素係「在實體環境或技術性事故中能夠及時回復個人資料可用性和存取之能力」。

Example

示例

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

控管者及其員工所使用的安全加密行動裝置遺失，無需通報監管機關。當加密金鑰保存在控管者安全擁有的範圍內，且遺失之個人資料並非唯一副本，侵害者將無法存取個人資料。此意味著侵害不太可能對相關當事人之權利和自由造成風險。若而後加密金鑰受到損害或加密軟體或演算法有漏洞之情事變得明顯，自然人權利和自由之風險將會改變，因此可能需要通報。

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have “default keys” that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years’ time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

然而，在資料實際上未被安全加密的情況下，若控管者未通報監管機關，則不符合第33條之規範。因此，在選擇加密軟體時，控管者應仔細評估該加密所提供之品質並正確的執行，並了解該加密軟體實際提供的保護層級以及是否適合可能之風險。控管者亦應熟悉其加密產品如何運作之細節。例如，設備可能在關閉後立即加密，但當其處於待機模式時則不加密。某些使用加密的產品具有「內建金鑰」，需要每位用戶更改後才會生效。也有可能該項加密(軟體)在當下會被安全專家認為是足夠的，但幾年後便過時，此意味該加密產品是否

可為資料提供充分加密和適當程度之保護即有疑問。

III. Article 34 – Communication to the data subject
第34條 – 與當事人之溝通

A. Informing individuals
通知當事人

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.
在某些情形下，除了通知監管機關外，控管者尚需向受影響之當事人就侵害進行溝通。

Article 34(1) states：
第34條第1項規定：

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."
> 「於個人資料侵害可能導致自然人權利和自由之高風險時，控管者應與當事人就個人資料侵害進行溝通，不得無故延遲。」

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.
控管者應記住，除非侵害不太可能對個人的權利和自由造成風險，否則向監管機關通報之義務為強制性。此外，若因侵害而可能導致個人之權利和自由面臨高風險時，則必須告知當事人。因此，向個人溝通侵害之門檻高於通報監管機關，所以並非所有侵害皆須與當事人溝通，從而保護其免受不必要的疲勞通知。

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to

provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.
GDPR規定「不得無故遲延」與當事人就侵害所進行之溝通，此意味著應儘快為之。通知當事人的主要目的係提供其有關自我保護所應採取措施之具體資訊[36]。如上所述，依據侵害之性質和所構成之風險，及時溝通將有助於當事人採取措施保護自己免受該侵害的任何負面影響。

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.
本指引的附錄B提供了一份清單列舉侵害何時可能導致當事人高風險之情況，以及控管者因此必須通知受影響個人之情形。

B. Information to be provided
所須提供之資訊

When notifying individuals, Article 34(2) specifies that：
在通知當事人時，第34條第2項規定：

> "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."
>
> 「本條第1項所稱與當事人之溝通，應以清楚簡易之語言描述個人資料侵害的性質，並至少包括第33條第3項第b、c、和d款中提及之資訊與措施。」

According to this provision, the controller should at least provide the following information：
依此規定，控管者至少應提供以下資訊：

- a description of the nature of the breach;
  侵害性質之描述；
- the name and contact details of the data protection officer or other contact point;
  個資保護長或其他聯絡點之姓名(名稱)和聯繫方式；

[36] See also Recital 86.
請另參閱前言第 86 點。

- a description of the likely consequences of the breach; and
  侵害可能之後果的描述；以及

- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
  控管者為解決侵害而採取或預計採取之措施的描述，若適當的話，則亦包括為減輕可能之不利影響而採取之措施。

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.
為解決侵害和減輕其可能的不利影響所採取之措施，例如，控管者可聲明，於向相關監管機關通報該侵害後，控管者已獲得有關管理該侵害及減輕其影響之建議。在適當的情況下，控管者亦應向當事人提供具體建議，使其得保護自己免受侵害可能產生之不利後果，例如當存取憑證受損時重置密碼。同樣地，控管者得選擇提供此處要求以外之資訊。

C. Contacting individuals
聯繫當事人

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).
原則上，應直接與受影響之當事人就相關之侵害進行溝通，除非此種溝通造成不成比例之付出。於此情形下，則應採取公眾溝通或類似措施，使當事人獲得同樣有效方式之通知（第34條第3項第c款）。

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.
在與當事人就侵害進行溝通時，應使用專用訊息，且不應與其他資訊(如定期更新、新聞通

訊或一般標準訊息)一併發送。此有助於使該溝通清晰透明。

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

透明溝通的方法包括如直接傳送訊息（例如，電子郵件、簡訊、直接訊息）、明顯的網站橫幅式廣告或通知、郵政通訊以及在印刷媒體中明顯的廣告。僅於新聞稿或在公司部落格上通知並非屬與當事人溝通侵害的有效方式。WP29建議控管者應選擇一種可使資訊傳達給所有受影響當事人之機會最大化。依據具體情況，這可能意味著控管者得採取多種溝通方式，而非僅使用單一接觸管道。

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

控管者可能亦需要確保溝通係以適當的替代形式和相關語言為之，以確保當事人能夠理解所提供之資訊。例如，在與當事人就侵害進行溝通時，使用和接收者在從前正常業務過程中所使用之語言通常是合適的。然而，若受侵害影響之當事人係控管者先前未曾與其進行過互動之個人，或特別是那些居住在控管者所在地以外之其他成員國或其他非歐盟國家之個人，在考量所需之資源，以當地國家之語言進行溝通是可接受的。關鍵在於協助當事人了解侵害之性質以及可採取保護自己之措施。

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the

breach as this channel could also be used by attackers impersonating the controller.
控管者最適合決定最適當的連繫管道，以與當事人就侵害進行溝通，特別是當控管者與客戶間有經常之互動情形。然而，顯然地，控管者應謹慎使用已受侵害之連繫管道，因為攻擊者亦可能冒充控管者使用該管道。

At the same time, Recital 86 explains that：
同時，前言第86點說明：

> "Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."
> 「此種與當事人之溝通應儘快在合理可行的情況下進行，且與監管機關密切合作，尊重監管機關或其他相關機關如執法機關提供之指導。例如，需降低損害之立即風險即須立刻與當事人溝通，而需實施適當措施以對抗持續的或類似的個人資料侵害則可使較長的溝通時間正當化。」

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.
因此，除了如何依據第34條通知當事人之建議外，控管者亦可能希望與監管機關連繫並諮詢有關發送適當訊息及聯繫當事人之最適方式的建議。

Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.
與前言第88點中之建議相連結，即侵害之通知應「考量執法機關的合法正當利益，當早期揭露可能會對個人資料侵害情形之調查造成不必要之妨礙」。這可能意味著在特定正當情形下，並依據執法機關之建議，控管者與受影響當事人就侵害之溝通得予延遲，直到不會

損害該調查為止。然而，其後仍需迅速通知該當事人。

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).
當儲存之資料不足以聯繫當事人，控管者則無法向該當事人就侵害進行溝通，在此特殊情形下，控管者應在溝通合理可行時，立即通知當事人(例如，當事人行使其第15條權利以近用個人資料並向控管者提供必要的附加資訊以便聯繫時)。

D. Conditions where communication is not required
不須溝通之情形

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are：
第34條第3項規定不須向當事人通知侵害的三種情形，包括：

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
  在侵害發生前，控管者對個人資料之保護已採取適當的技術性與組織性措施，特別是使未獲授權存取之人無法解讀個人資料之措施。例如，可能包括使用最先進之加密或透過代碼化(tokenization)來保護個人資料。

- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals’ rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
  在侵害發生後，控管者立即採取措施確保個人權利和自由之高風險已不再可能實現。例如，依據案件具體情況，在存取個人資料者進行任何操作之前，控管者或許已立即辨別出並對其採取行動。仍須適當考量任何保密性之侵害可能的結果，

同樣地，此須取決於相關資料之性質。

- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

  若聯繫當事人可能造成不符比例之付出[37]，或因侵害而遺失聯繫方式或從一開始便不知悉聯繫方式。例如，統計辦公室的倉庫被淹沒，而包含個人資料之文件僅以紙本形式儲存。控管者必須採取公眾溝通或類似措施替代，以同樣有效之方式通知當事人。在不成比例之付出情況下，控管者可設想以技術性之安排，依需求提供侵害之資訊，這對可能受侵害影響卻無法聯繫之當事人有所助益。

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

依據課責原則，控管者應要能夠向監管機關證明其符合一種或多種之情形[38]。仍須記住，雖然因為對自然人的權利和自由無風險之存在，最初也許不需要通知，但這或許會隨著時間的推移而發生變化，並必須重新評估風險。

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850
請參閱 WP29 關於透明化之指引，該指引將考量不成比例付出之議題，請查閱：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850。

[38] See Article 5(2)
請參閱第5條第2項。

employing its available powers and sanctions.

若控管者決定不向當事人就侵害進行溝通，第34條第4項說明，當監管機關認為該侵害可能會對個人造成高風險，監管機關可要求控管者為之。又或監管機關認第34條第3項之要件已被滿足，在此情形下則不需要通知當事人。若監管機關認為不通知當事人之決定並無充分依據，得考量採取其可使用之權力和裁罰。

IV. Assessing risk and high risk
風險和高風險之評估

A. Risk as a trigger for notification
風險為觸發通知之要件

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances：

雖然GDPR採用了侵害通知之義務，但該義務並非適用於所有情況：

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
  除非侵害不太可能對個人之權利及自由造成風險，否則必須通報權責監管機關。

- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.
  只有在可能對其權利和自由造成高風險之情況下才會觸發與當事人就侵害進行溝通之義務。

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this： firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

這表示一旦知悉侵害，控管者不僅應該設法控制事故，還應該評估該事件可能導致之風險，這一點非常重要。此包含兩項重要原因：第一，瞭解對個人影響之可能性和潛在嚴重程度將有助於控管者採取有效措施來控制和解決侵害；第二，這將有助於決定是否需通報監管機關，並在必要時通知相關當事人。

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

如上所述，除非不太可能對個人之權利及自由造成風險，否則必須通知侵害，且需要向當事人就侵害進行溝通之關鍵觸發要件為對個人之權利和自由造成*高*風險之可能。此種風險存在於當侵害可能導致資料被破壞之當事人遭受人身、財物或非財物的損害。損害之示例包括歧視、冒用身分或詐欺、財務損失和聲譽受損。當侵害涉及揭露種族或民族血統、政治觀點、宗教或哲學信仰或公會會員資格之個人資料，或包括基因資料、有關健康之資料或有關性生活之資料，或前科及犯罪或相關安全措施，此時應被認定有損害發生之可能[39]。

B. Factors to consider when assessing risk

風險評估考量之要件

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

GDPR前言第75點和第76點建議，通常在評估風險時，應考量當事人之權利和自由所受風險的可能性和嚴重性。前言進一步指出，風險應在客觀評鑑基礎上為之。

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

[39] See Recital 75 and Recital 85.
請參閱前言第75點及前言第85點。

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.
請參閱 WP 關於 DPIA 之指引：http://ec.europa.eu/newsroom/document.cfm?doc_id=44137。

應該注意到，評估因侵害而對個人權利和自由所造成之風險與個資保護影響評估(DPIA)[40]中考量之風險所關注的重點不盡相同。DPIA同時考量按計畫進行資料運用之風險，以及若發生侵害之風險。在考量潛在的侵害時，DPIA概括性的著重在發生此類情形之可能性，以及對當事人可能發生之損害；易言之，這是對假設事件之評估。就實際之侵害而言，由於事件已經發生，因此完全著重於侵害對個人造成之影響。

Example

示例

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

DPIA建議，預計使用特定安全軟體產品來保護個人資料是一種合適的措施，以確保因運用程序對個人造成之風險有適當的安全層級。然而，若隨後始知悉漏洞，這將改變該軟體控制受保護的個人資料風險之合適性，因此作為進行中的DPIA的一部分，須重新評估。

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

產品中之漏洞隨後被利用，並發生侵害。控管者應評估侵害之具體情況、受影響之資料、對個人的潛在影響程度、以及該風險實現之可能性。

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]：

因此，在評估因侵害導致的個人風險時，控管者應考量侵害之具體情況，包括潛在影響的嚴重程度以及該情況發生之可能性。因此，WP29建議評估應考量以下標準[41]：

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR.
See http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
611/2013 規則第 3.2 條為電子通訊服務業就侵害通知應考量之要素提供指導，該指導可能對 GDPR 下關於通知之義務有所助益。請查閱:
http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF。

- The type of breach
  侵害之類型

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual’s medical details have been lost, and are no longer available.
已發生之侵害類型可能會影響對個人造成風險之程度。例如，在機密性之侵害中，醫療資訊被揭露予未授權之人對個人所造成之後果，應與個人詳細醫療資料遺失且無法再使用之情況不同。

- The nature, sensitivity, and volume of personal data
  個人資料之性質、敏感性和數量

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.
當然，在評估風險時，關鍵因素是受侵害影響的個人資料之類型和敏感性。通常，資料越敏感，被影響之當事人受到傷害之風險就越高，但仍應考量已可使用的有關當事人的其他個人資料。例如，在一般情況下，揭露個人姓名和地址不太可能造成實質的損害。然而，若將養父母之姓名和地址透露予親生父母，則對養父母和子女造成之後果可能非常嚴重。

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.
涉及健康資料、身分證明文件或財務資料（如信用卡詳細資訊）之侵害本身皆可造成傷害，若將資料一併使用，則可能會被用於冒用身分。個人資料之組合通常比單項個人資料更為敏感。

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have

requested that their deliveries be stopped while on holiday would be useful information to criminals.
某些類型的個人資料最初可能相對無害，然而，應仔細考量該資料可能揭露受影響個人之程度。一份接受定期遞送的客戶列表可能並非特別敏感，但是同樣的資料，若是關於客戶要求在休假期間停止遞送，對於犯罪分子來說則是有用之資訊。

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.
同樣的，少量卻高度敏感之個人資料可能對個人產生重大影響，且大量的詳細資料可能揭露關於該個人更大範圍的資訊。此外，當侵害影響許多當事人之大量個人資料時，該侵害會對相對應之大量個人產生影響。

- Ease of identification of individuals
  識別個人之容易度

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.
需考量的一項重要因素為，對能夠存取受侵害個人資料之一方而言，其可識別特定個人或以資料與其他資訊進行對照以識別個人之容易程度為何。依據具體情況，也許可直接從受侵害之個人資料進行識別，而無需特殊研究便可辨別個人身分，又或將個人資料與特定個人對照也許非常困難，但在某些條件下仍有可能為之。從受侵害之資料中可能直接或間接識別個人，能否識別也可能與侵害之具體背景及相關個人詳細資訊的公開可得性相關。此處可能與機密性和可用性之侵害更為相關。

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data

subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.
如上所述，受到適當加密程度保護的個人資料對於沒有解密金鑰之未經授權人而言是無法解讀的。此外，適當採用假名化(第4條第5款將其定義為「運用個人資料之方式，即個人資料在不使用額外資訊時，無法識別出特定之當事人，且該額外資訊已被分開保存，並以技術性與組織性措施確保該個人資料無法顯示已識別或可識別之自然人」)亦可降低在發生侵害時識別個人之可能性。然而，單獨使用假名化技術不能被認作使資料無法解讀。

- Severity of consequences for individuals
  對當事人造成之嚴重後果

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.
依據侵害所涉及個人資料之性質，例如特殊類別之資料，對個人造成的潛在損害可能格外嚴重，特別是在該侵害會導致身分遭冒用或詐欺、身體傷害、心理困擾、羞辱或損害名譽之情況時。若侵害涉及弱勢群體之個人資料，可能會使他們置身於更大的損害風險中。

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the

controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).
控管者是否知悉個人資料掌握在意圖不明或可能為惡意之人的手中，會影響潛在風險之程度。當向如第4條第10款所定義之第三方或其他錯誤之接收者揭露個人資料時，則可能會有機密性侵害。例如，可能發生個人資料意外傳送至組織的錯誤部門或常用的供應商。控管者可能要求接收者返還或安全地銷毀所接收之資料。在此二情形下，因控管者與錯誤的接收者有持續性之關係，並可能知悉其程序、歷史和其他相關細節，因此可認定該接收者為「可信任的」。也就是說，控管者對該接收者可能具有一定程度的確信，可以合理期待該接收者不會閱讀或存取錯誤發送之資料，並遵守返還該資料之要求。即使已存取了資料，控管者仍可能信任接收者不會對該資料採取任何進一步之操作，並立即將資料返還給控管者且與其合作回復資料。在此情形下，這可能會成為控管者在侵害發生後進行風險評估中的要素之一：接收者係可信任的事實可能會消除侵害後果之嚴重性，但並不意味著沒有侵害之發生。然而，這可能會去除個人風險的可能性，因此不再需要通報監管機關或受影響之當事人。同樣地，這將取決於具體個案情況。儘管如此，作為保存侵害記錄之一般義務的一部分，控管者仍必須保留侵害之相關紀錄（請參閱下文第V節）。

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.
另應考量對個人造成後果之持續性，若影響為長期性，則可能會認為衝擊較大。

- Special characteristics of the individual
  當事人之特點

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.
侵害可能會涉及有關兒童或其他弱勢者之個人資料，使其面臨更高之危險風險。尚存在關於當事人之其他因素可能影響侵害對其造成衝擊之程度。

- Special characteristics of the data controller
  資料控管者之特點

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
控管者的性質和角色與其活動，可能會影響因侵害而對個人造成風險之程度。例如，醫療機構運用特種個人資料，意味著若該個人資料遭受侵害，相較於報紙的郵寄名單而言，將會對當事人造成更大之風險。

- The number of affected individuals
  受影響當事人之數量

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.
侵害可能影響一個人、少數人或數千人。一般來說，受影響當事人越多，侵害造成的衝擊就越大。然而，依個人資料之性質與其受損害之情況，侵害甚至可能僅對一個人產生嚴重的影響。同樣地，關鍵是要考量對受影響個人造成衝擊之可能性和嚴重性。

- General points
  一般要點

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.
因此，在評估可能因侵害而造成之風險時，控管者應同時考量對當事人權利和自由潛在影響之嚴重程度以及該影響發生之可能性。顯然地，若侵害之後果越嚴重，風險就越高，同樣地，當發生的可能性越大，風險也會提高。若有疑問，控管者應謹慎行事並進行通知。

附錄B提供了一些不同類型之侵害所涉及當事人風險或高風險的有用範例。

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].
歐盟網路和資訊安全局（ENISA）就評估侵害嚴重性之方式提出了建議，這對控管者和受託運用者在設計侵害管理應變計畫時也許有所助益[42]。

V. Accountability and record keeping
歸責和紀錄之保存

A. Documenting breaches
記錄侵害事件

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains：
無論侵害是否需要通報監管機關，控管者必須留存所有侵害之紀錄，如第33條第5項所述：

> “The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.”
> 「控管者應記錄任何個人資料侵害事件，包括與個人資料侵害相關之事實、其影響和所採取之補救措施。該紀錄應使監管機關得以確認是否符合本條。」

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller’s obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity
ENISA，關於評估當事人資料侵害嚴重性方法之建議，請查閱：https://www.enisa.europa.eu/publications/dbn-severity。

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.
控管者可以選擇將記錄侵害作為其依據第 30 條保存運用活動紀錄之一部分。若可清楚識別與侵害相關之資訊，並可根據要求提取，則不需要分別登記。

這可連結至GDPR第5條第2項所規範之課責原則。記錄不須通報之侵害的目的與應通報之侵害的目的一樣，與第24條之控管者義務相關，且監管機關可要求查看該紀錄。因此，無論是否需要通報，鼓勵控管者建立內部侵害登記制度[43]。

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.
雖然係由控管者決定在記錄侵害時所使用之方法和結構，但就可記錄之資訊而言，有適用於所有情況之關鍵要素。依據第33條第5項之規定，控管者需記錄關於侵害之詳細資訊，其中應包括侵害之原因、發生之事件以及受影響之個人資料。亦應包含侵害之影響與後果，以及控管者所採取之補救措施。

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.
GDPR並未規定此類紀錄的保留期間。若此類紀錄包含個人資料，則控管者有責任依據與個人資料運用有關之原則[44]決定適當的保留期限，並符合合法運用之要件[45]。控管者需依據第33條第5項保留紀錄，當監管機關要求時，做為遵循該條規定或符合課責原則之證據。顯然地，若紀錄本身不包含個人資料，則不適用GDPR的儲存限制原則[46]。

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers

[44] See Article 5.
請參閱第5條。
[45] See Article 6 and also Article 9.
請參閱第6條及第9條。
[46] See Article 5(1)(e).
請參閱第 5 條第 1 項第 e 款。

the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.
除這些細節外，WP29亦建議控管者記錄其就侵害所做決定之理由。特別是，若未通報該項侵害，該決定之正當性應予記錄。這應包括控管者認為該侵害不太可能對個人權利和自由造成風險之原因[47]。或者，若控管者認為已符合第34條第3項中之任何要件，則應能夠提供適當證據證明之。

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.
當控管者確實向監管機關通報侵害，但該通報是遲延的，則控管者必須能夠提供遲延之理由；與此相關之紀錄有助於彰顯該遲延通報係正當且非過度的。

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.
當控管者向受影響之當事人就侵害進行溝通時，關於該侵害(相關內容)應透明，並以且有效之方式進行。因此，藉由保留此類溝通之證據，將有助於控管者彰顯其課責性和合規。

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.
為協助遵循第33條和第34條之規定，若控管者和受託運用者皆執行通報程序記錄，列出在偵測到侵害後所應遵循之流程，包括如何控制、管理和修復該事件，以及評估風險和通報該侵害。就此，可展現其遵循GDPR，並可能有助於說明員工已被告知此類程序和機制之存在，並知悉如何應對侵害之發生。

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with

[47] See Recital 85
請參閱前言第 85 點。

Article 83.
另應注意，未妥善記錄侵害將使監管機關得依據第58條行使其權力，及/或依據第83條處以行政罰鍰。

B. Role of the Data Protection Officer

個資保護長之角色

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.
控管者或受託運用者可依據第37條之要求或出於自願性的良好實踐指派個資保護長（DPO）[48]。GDPR第39條規定一些DPO之強制性任務，但於適當情形下，並不妨礙控管者分配其他任務予DPO。

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.
DPO的強制性任務中與侵害通報特別相關者，包括向控管者或受託運用者提供資料保護建議和資訊、監控對GDPR的遵循及提供與DPIA相關之建議。DPO亦須與監管機關合作，並作為監管機關和當事人之聯絡點。另須注意，第33條第3項b款要求於向監管機關通報侵害時，控管者應提供其DPO或其他聯絡點之名稱和詳細聯繫方式。

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.
就侵害之記錄而言，控管者或受託運用者可能希望獲得DPO就關於該紀錄的結構、設置和管理方面之意見。DPO還可能被額外指派負責維護這些紀錄之任務。

These factors mean that the DPO should play an key role in assisting the prevention of or

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
請參閱 WP 有關 DPO 之指引文件: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083。

preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

這些要素意味著DPO應透過提供建議和監督合規性，在協助防止侵害或侵害之因應準備、與侵害期間(即通報監管機關時)及任何後續監管機關的調查期間，扮演關鍵角色。有鑑於此，WP29建議應迅速通知DPO侵害之存在，並使其參與整個侵害管理和通報之程序。

VI. Notification obligations under other legal instruments 其他法律文件下之通報義務

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following：

除了依據GDPR通報和溝通侵害之義務外，控管者亦須知悉依據其他可能適用的相關法律就通報安全事件之任何要求，以及是否可能也同時要求他們就個人資料侵害之情事通報監管機關。該要求可能因成員國而異，但其他法律文件規定之通報要求及其如何與GDPR相互關連之示例如下：

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

(EU)910/2014 關於歐盟內部市場電子交易之電子識別和信賴服務規則（eIDAS規則）[49]。

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

eIDAS規則第19條第2項要求信賴服務提供者，當其遭受之安全侵害或信賴喪失會對所提供

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG 請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG。

之信賴服務或其所保存之個人資料產生重大影響時，應通報其監管部門。而在適用之情形下 - 即若此類侵害或損失亦屬GDPR下之個人資料侵害時 - 信賴服務提供者亦應通報監管機關。

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

（EU）2016/1148關於跨歐盟網路與資訊系統高度共同安全措施指令（NIS指令）[50]。

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

NIS指令第14條和第16條要求基本服務運營商和數位服務提供者向其權責機關通報安全事故。依據NIS前言第63點[51]，安全事故通常會包含個人資料之侵害。雖然NIS要求權責機關和監管機關合作並交換資訊，但若該類事件是/或成為GDPR下之個人資料侵害，則該運營商和/或提供者可能被要求與NIS要求之事故通報分開，另行通報監管機關。

Example

示例

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

若侵害事件包括個人資料侵害，雲端服務提供者依據NIS指令通報侵害時，可能亦需通知控管者。同樣的，在侵害發生時，信賴服務提供者依據eIDAS通報侵害事件時，亦有可能被要求通報相關個人資料保護機關。

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
請參閱 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG。

[51] Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*
前言第 63 點:「*在許多案例中，個人資料會因事故而受到損害。在此情形下，權責機關和資料保護機關應合作並交換所有相關事項之資訊，以解決因事故而導致的任何個人資料侵害。*」

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).
  2009/136/EC指令（公民權利指令）和 611/2013規則（侵害通知規則）。

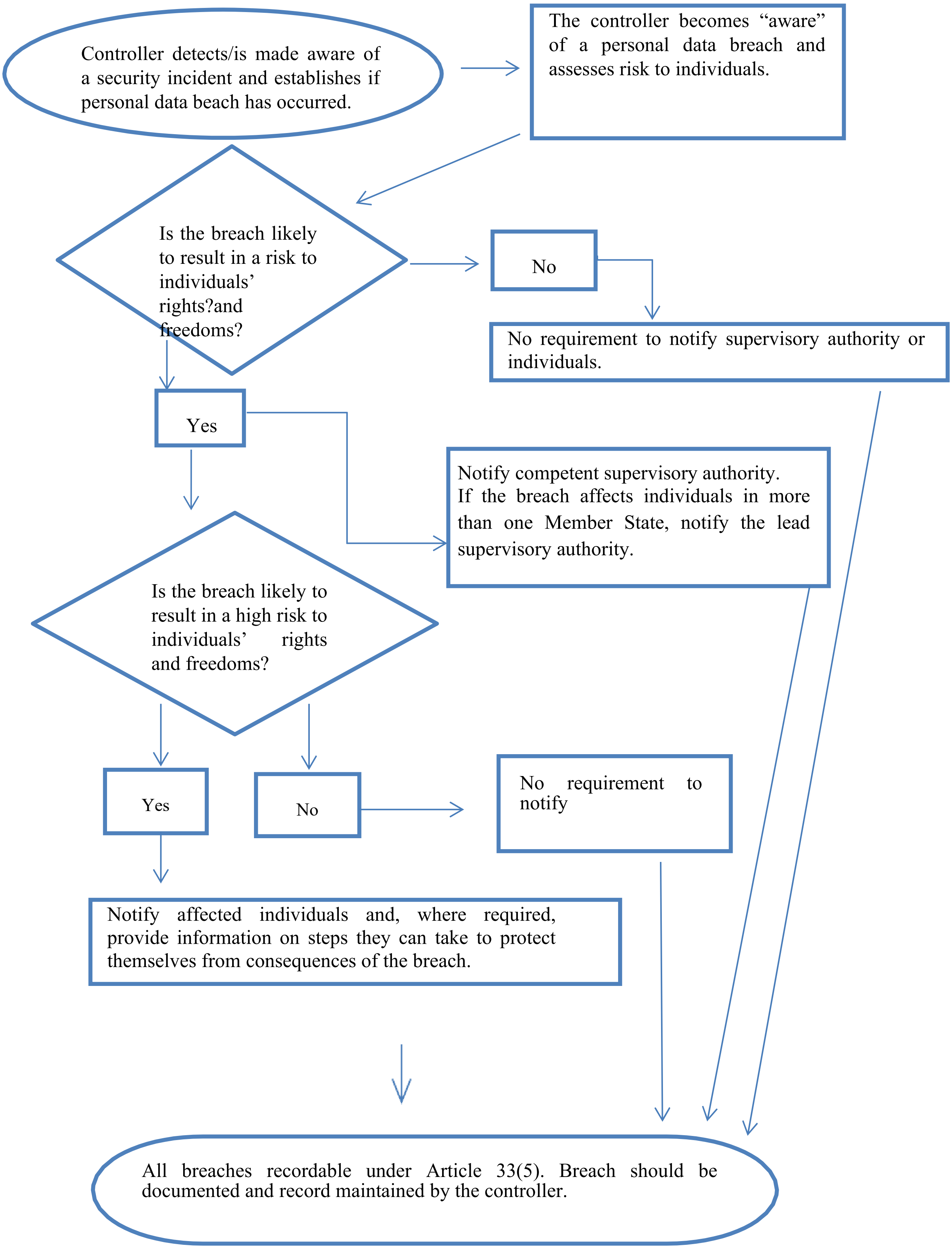
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52]must notify breaches to the competent national authorities.
在2002/58/EC[52]指令中所指之公眾電子通信服務提供者必須將侵害通報權責國家機關。

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.
控管者亦應知悉於其他可適用制度下之任何額外法律、醫療或專業之通知責任。

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, seehttps://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
2017 年 1 月 10 日，歐盟執委會提出了一項關於隱私權和電子通訊規則，此將取代 2009/136/EC 指令並刪除通知之要求。然而，在歐洲議會批准該提案前，現有之通知要求仍屬有效，請參閱:
https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications。

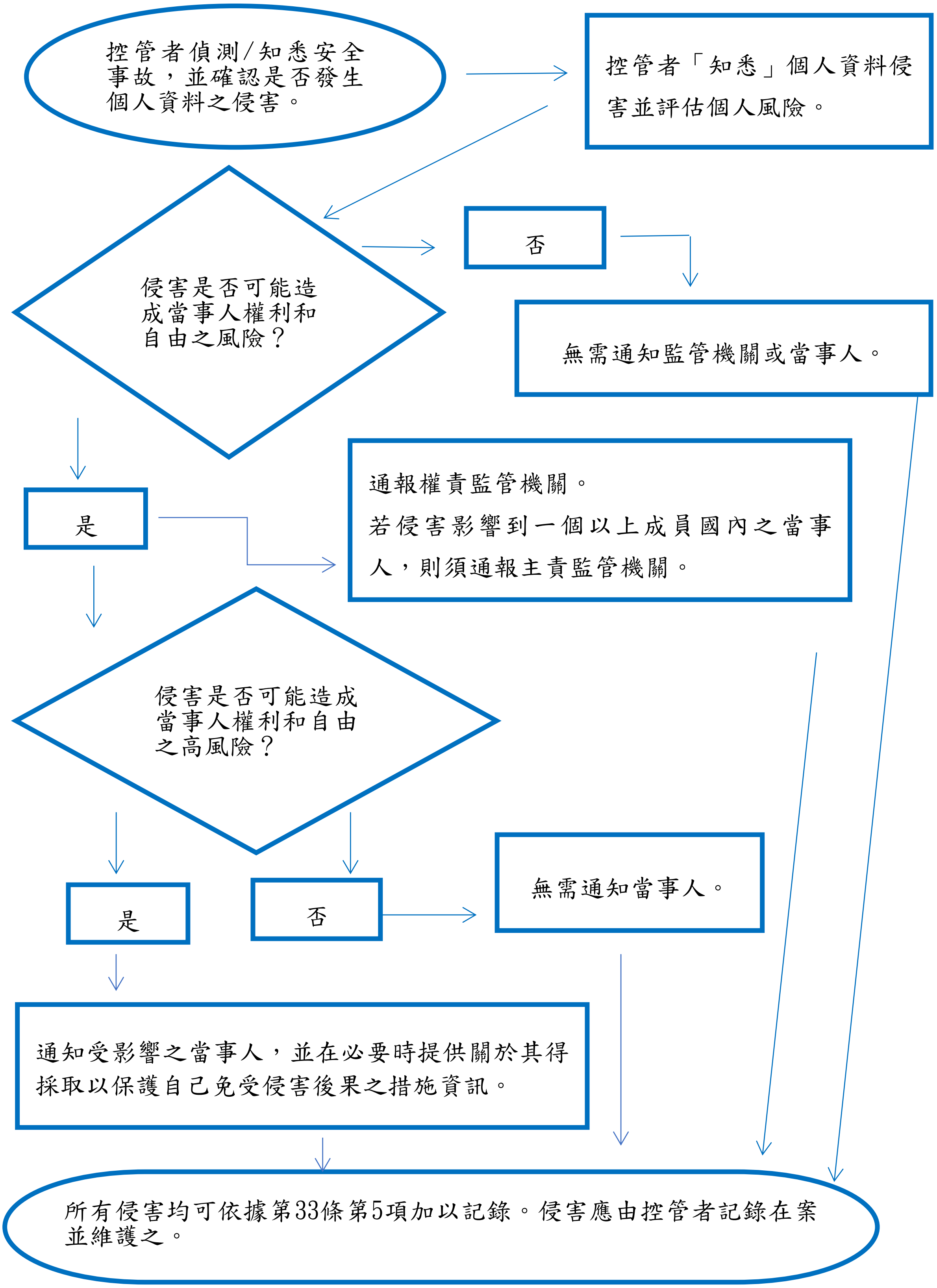
VII. Annex

A. Flowchart showing notification requirements


Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.
The controller becomes “aware” of a personal data breach and assesses risk to individuals.
Is the breach likely to result in a risk to individuals’ rights?and freedoms?
No
No requirement to notify supervisory authority or individuals.
Yes
Notify competent supervisory authority. If the breach affects individuals in more than one Member State, notify the lead supervisory authority.
Is the breach likely to result in a high risk to individuals’ rights and freedoms?
Yes
No
No requirement to notify
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.
All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

VII. 附錄

A. 通知要求流程圖


控管者偵測/知悉安全事故，並確認是否發生個人資料之侵害。
控管者「知悉」個人資料侵害並評估個人風險。
侵害是否可能造成當事人權利和自由之風險？
否
無需通知監管機關或當事人。
是
通報權責監管機關。
若侵害影響到一個以上成員國內之當事人，則須通報主責監管機關。
侵害是否可能造成當事人權利和自由之高風險？
是
否
無需通知當事人。
通知受影響之當事人，並在必要時提供關於其得採取以保護自己免受侵害後果之措施資訊。
所有侵害均可依據第33條第5項加以記錄。侵害應由控管者記錄在案並維護之。

B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.

iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a

			digital service provider.
vii. A website hosting company acting as data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigations the affected controllers should be reasonably confident as to whether each has suffered a breach and thereof is likely to be considered as having “become aware” once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individual they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient’s well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the “to：” or “cc：” fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist)	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

	or if other factors present high risks (e.g. the mail contains the initial passwords).		

B. 個人資料侵害示例及應通報(知)之對象

以下非完全列舉之示例將協助控管者決定在不同的個人資料侵害情況下是否需要進行通知。這些示例也可能有助於區分對個人權利和自由之風險及高風險。

示例	是否通報監管機關？	是否通知當事人？	注意事項/建議
i. 控管者將個人資料之備份檔案儲存在加密的USB智能儲存裝置上。該裝置因竊盜闖入而遭偷竊。	否。	否。	只要資料是以最先進的演算法進行加密、資料備份仍存在該特定金鑰未受到損害，且資料可於適當時機回復時，則可能不屬於需要通報之侵害。 然而，若其後遭受損害，則需要通報。
ii. 控管者維護一個線上服務。由於對該服務的網路攻擊，致使當事人的個人資料外洩。 該控管者僅在歐盟單一成員國境內擁有客戶。	是，若對當事人可能產生後果，應通報監管機關。	是，依據受影響個人資料之性質以及對當事人權利可能造成後果之嚴重性，通知該當事人。	
iii. 控管者電話服務中心短暫停電幾分鐘，意味著客戶無法致電控管者並存取其紀錄。	否。	否。	此非屬須通知之侵害，但仍屬於第33條第5項規定下可記錄之事故。控管者應保存適當之記錄。
iv. 控管者遭受勒索軟體攻擊，導致所有資料皆被加密。無可用之備份，亦無法回	是，若可能對當事人產生後果，需通報監管機構，因其屬於可用性喪失之侵害。	是，依據受影響個人資料之性質以及無法獲取資料可能產生之影響，以及	若有可用之備份且資料可適時回復，則不需要通報監管機關或當事人，因此處並無永久

復資料。在調查中發現，很明顯勒索軟體的唯一功能是加密資料，且系統中不存在其他惡意軟體。		其他可能之後果，通知當事人。	的可用性或機密性之損失。 然而，若監管機關透過其他方式知悉該事故，得考慮進行調查，以評估是否符合第32條中更廣泛之安全要求。
v. 某人致電給銀行的電話服務中心告知資料侵害事件。該個人收到其他人的月結單。 控管者進行了簡短的調查（即在24小時內完成），並合理確信已發生個人資料之侵害，以及是否存在系統性缺陷，可能意味著其他人受到或可能受到影響。	是。	若存在高風險且明顯地並無其他人受到影響，則僅需通知受影響之當事人。	若在進一步調查後發現有更多人受到影響，則必須向監管機關更新通報，且若對其他人存在高風險時，控管者需要採取額外步驟，對他人進行通知。
vi. 控管者經營一個網路賣場，並在多個成員國皆擁有客戶。該賣場遭受網路攻擊，且攻擊者在網路公布用戶名稱、密碼和購買歷史記錄。	是，若涉及跨境運用，通知主責監管機關。	是，因其可能造成高風險。	控管者應該採取行動，例如透過強制重置受影響帳戶之密碼，以及其他降低風險之措施。 控管者尚應考量任何其他通知義務，例如：作為NIS指令中數位服務提供者之義務。

vii. 擔任資料受託運用者之網站託管公司發現控制用戶授權之程式碼有錯誤。該錯誤之影響意味著任何用戶皆可存取任何其他用戶的帳戶詳細資訊。	作為受託運用者，網站託管公司必須通知其受影響之客戶（控管者），不得無故遲延。 假設網站託管公司已自身進行了調查，受影響之控管者應對是否遭受侵害有合理之確信，因此一經託管公司（受託運用者）通知，即可被視為「知悉」。控管者因而必須通報監管機關。	若對當事人沒有造成高風險之可能，則不需通知。	網站託管公司（受託運用者）必須考量任何其他通知義務（例如，作為NIS指令中數位服務提供者之義務）。 若無證據表明此錯誤被其任何控管者利用，則可能沒有發生須通知之侵害，但仍可屬於係可記錄之侵害，或是屬於第32條中不合規之情形。
viii. 由於網路攻擊，醫院病歷在30小時內無法使用。	是，基於對患者健康與隱私之高風險，醫院有義務通報。	是，須通知受影響之當事人。	
ix. 大量學生的個人資料被錯誤地發送到有1000多個收件人之錯誤郵件列表。	是，須通報監管機關。	是，依據所涉及個人資料之範圍和類型以及可能後果之嚴重程度，通知當事人。	
x.行銷電子郵件將收件人郵件放置在正本收件人「to：」或副本收件人「cc：」中，因此每個收件人都可看到其他收件人之電子郵件地址。	是，若大量當事人受到影響；或若敏感資料遭揭露（例如心理治療師之郵件列表）；或其他存在高風險之因素（例如包含原始密碼之郵件），通報監管機關則可能是強制性的。	是，依據所涉及個人資料之範圍和類型以及可能後果之嚴重程度，通知當事人。	若未揭露敏感資料且僅有少量電子郵件地址遭揭露，則可能不需要通知。