仮日本語訳

Guidelines on Personal data breach notification under Regulation
規則に基づく個人データ侵害通知に関するガイドライン

本書面は、ARTICLE 29 DATA PROTECTION WORKING PARTY （第29条作業部会）により2017年10月3日に採択後、修正のうえ2018年2月6日に採択された、 “Guidelines on Personal data breach notification under Regulation” の英語版の一部を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。

TABLE OF CONTENTS

目次

INTRODUCTION
序

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.
一般データ保護規則（GDPR）は、個人データの侵害（以下「侵害」とする）を国内の所轄監督機関[1]（越境侵害の場合は、主監督機関）に通知すること、また特定の場合においては、侵害により個人データが影響を受けている個人に通知する要件を導入している。

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
GDPR の第 4 条(21)参照
[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
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 及び http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611 参照
[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm 参照
[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 参照
[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
欧州連合基本権憲章において保障されている権利は、以下から閲覧可能
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.
第 33 条(2)参照。これは、個人データの侵害が生じた場合に、（契約者と直接的な契約関係を締結せずに）電子通信サービスの一部を提供することを契約しているプロバイダーに、契約プロバイダーへの通知を義務付けることを定める(EU)規則 No 611/2013 の第 5 条の概念に類似している。

公に入手可能な電子通信サービスのプロバイダー等の一定の組織については、侵害が生じた場合の通知義務が現に定められている（指令 2009/136/EC 及び（EU）規則 No. 611/2013 に規定）[2]。既に、独自の国内侵害通知義務を定めている EU 加盟国もある。公に入手可能な電子通信サービスのプロバイダーに加えて、管理者に分類される組織が関与する侵害通知義務（例：ドイツ及びイタリア）や、個人データが関与するすべての侵害を報告する義務（オランダ等）を定めているものもある。関連実施規範（アイルランド等[3]）を定めている加盟国もある。現在、複数の EU データ保護機関が、侵害の報告を管理者に勧告しているが、GDPR に代替されるデータ保護指令 95/46/EC[4]は、特定の侵害通知義務を定めていないため、かかる通知要件は、多くの組織にとって新たな要件となる。現在 GDPR は、侵害が個人の権利及び自由に対するリスクに帰結する可能性が低い場合を除き、すべての管理者に対し通知を強制している[5]。処理者もまた、重要な役割を担っており、その管理者に対し侵害を通知しなければならない[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.

第 29 条作業部会（WP29）は、新たな通知要件には多くの利点があると思慮している。管理者は、監督機関に通知する際、影響を受ける個人に通知する必要があるか否かについて助言を得ることができる。実際、監督機関は、侵害について当該個人に通知することを管理者に命令することができる[7]。侵害について個人に連絡することにより、管理者は、侵害の結果生じるリスク及び当該個人が潜在的リスクから自己防衛するために講じることのできる措置について情報を提供することが可能になる。侵害対応計画は、個人及びその個人データの保護に焦点を当てるべきである。よって、侵害の通知は、個人データの保護に関する規則の遵守を強化するツールとみなされるべきである。同時に、個人又は監督機関への侵害の報告を怠ると、第 83 条に基づき、何らかの制裁が管理者に適用される場合があることに留意しておくべきである。

[7] See Articles 34(4) and 58(2)(e)
第 34 条(4)及び 58 条(2)(e)参照

Controllers and processors are therefore encouraged to plan in advance and put in place processes 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.
よって、管理者及び処理者は、侵害を検知して速やかに阻止し、個人に対するリスクを評価し[8]、その後に所轄監督機関への通知の要否を判断し、必要に応じて関連する個人に侵害を報告することを可能にする工程を事前に計画し、確立しておくことが推奨される。監督機関への通知はインシデント対応計画の一部を成すものでなければならない。

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 は、侵害を通知する必要がある場合はいつか、誰に通知すべきか、また通知の一環としてどのような情報を通知すべきかについての定めを含んでいる。通知が求められる情報は、段階的に提供することができるが、いかなる場合においても、管理者は、すべての侵害に対し迅速に対応すべきである。

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.
第 29 条作業部会は、個人データ侵害の通知に関する Opinion 03/2014[9] において、侵害が生じた場合にデータ主体に通知すべきか否を判断する際に参考となる指針を管理者に提供した。本意見書は、指令 2002/58/EC に関する電子通信サービスのプロバイダーの義務を考察し、その時点における GDPR 草案に照らし、複数の産業分野における例を挙げ、すべての管理者に対する望ましい慣行を提示している。

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.

---

[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).
かかる措置は、自然人の権利及び自由に対しリスクが発生する可能性の高い処理作業に対し求められる、DPIA の監視及びレビュー要件に基づき確保することができる（第 35 条(1)及び(11)）。

[9] See Opinion 03/2014 on Personal Data Breach Notification
個人データの侵害通知に関する意見 03/2014 参照
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

現行のガイドラインは、GDPR の義務である侵害通知及び報告要件、並びにかかる新たな義務を遵守するために管理者及び処理者が講じ得る措置について説明している。また、多種類の侵害例及び多様な状況下において誰に侵害を通知すべきかを例示している。

I. Personal data breach notification under the GDPR
I. GDPR に基づく個人データ侵害通知

A. Basic security considerations
A. 安全に関する基本的な考慮事項

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 は、適切な技術的かつ組織的対策により、個人データの不正又は違法な取扱いからの保護及び偶発的な喪失、破壊又は破損 [10] からの保護を含め、個人データの適切なセキュリティを確保できる方法で個人データを取扱うことを要件の一つとしている。

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].
よって、GDPR は、取り扱われる個人データがさらされるリスクに対し、一定レベルの適切なセキュリティを担保できる適切な技術的かつ組織的な対策を確立することを、管理者及び処理者の両者に求めている。管理者及び処理者は、取扱いの最先端技術、実施費用、性質、範囲、コンテクスト及び目的、並びに発生確率及び深刻度の異なる自然人の権利及び自由に対するリスクを考慮すべきである [11]。また、GDPR は、侵害が生じたか否かを速やかに確証し、通知義務が関与するか否かを判断するための [12]、あらゆる適切な技術的保護及び組織的対策を確立することを求めている。

[10] See Articles 5(1)(f) and 32.
第 5 条(1)(f)及び第 32 条参照
[11] Article 32; see also Recital 83
第 32 条、前文第 83 項も参照
[12] See Recital 87
前文第 87 項参照

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.
よって、すべてのデータセキュリティポリシーの主要要素は、可能な限り侵害の発生を防止し、それにもかかわらず侵害が生じた場合は、迅速に対応することができることである。

B. What is a personal data breach?
B. 個人データの侵害とは

1. Definition
1. 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:
データ侵害に対処する試みの一環として、管理者は、まず、侵害を認識できなければならない。GDPR は、第 4 条(12)において「個人データの侵害」を下記のように定義している。

> "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."
> 「偶発的又は違法な、破壊、喪失、改変、無権限の開示又は無権限のアクセスを導くような、送信され、記録保存され、又は、その他の取扱いが行われる個人データの安全性に対する侵害」

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.
個人データの「破壊（destruction）」が何を指すのかは、比較的明白と言える。これは、データが存在しなくなる場合又は管理者にとって使用可能な形式で存在しなくなる場合を意味する。「破損（damage）」という文言も、比較的明白と言える。これは、個人データが変更若しくは損傷されること、又は完全な状態でなくなることを意味する。個人データの「喪失（loss）」とは、データが依然として存在する可能性があるが、管理者が当該データを制御できなくなった場合若しくは当該データにアクセスできなくなった場合、又は当該データが管理者の所有下に存在しなくなった場合と解釈すべきである。最後に、不正又は違法な取扱いには、データの受領権限を持たない取得者への個人データの開示（又はかかる取

得者による当該データへのアクセス）又は GDPR を違反するその他の形式の取扱いが含まれうる。

Example
事例
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.
個人データの喪失の例には、管理者の顧客データベースのコピーを包含する装置が紛失した又は盗難にあった場合が含まれる。また、個人データセットのコピーのみがランサムウェアにより暗号化された場合又は管理者が暗号化に用いたキーを失った場合も、データ喪失の例に挙げられる。

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].
侵害は、一種のセキュリティインシデントであることを明白にしておくべきであるが、第 4 条(12)に示唆されているように、GDPR は、*個人データ*の侵害が発生した場合のみ適用される。かかる侵害により、管理者は、GDPR の第 5 条に概略されている個人データの取扱いに関する原則の遵守を確保できなくなる。このことは、セキュリティインシデントと個人データ侵害の違いを明示している。つまり、個人データの侵害は、すべてセキュリティインシデントであるのに対し、セキュリティインシデントは、必ずしもすべて個人データの侵害であるとは限らないのである [13]。

The potential adverse effects of a breach on individuals are considered below.
侵害が個人に与えうる悪影響を以下に考慮する。

2. Types of personal data breaches
2. 個人データ侵害の種類

[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.
セキュリティインシデントは、外部ソースにより組織が攻撃される脅威モデルに限られず、セキュリティー原則を違反する内部取扱いに起因するインシデントが含まれることに留意すべきである。

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]:
第 29 条作業部会は、侵害の通知に関する意見 03/2014 において、侵害は、広く認知されている下記三点の情報セキュリティ原則に従い分類できることを説明した [14]。

・“Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.
・“Integrity breach” - where there is an unauthorised or accidental alteration of personal data.
・“Availability breach” - where there is an accidental or unauthorised loss of access[15] to, or destruction of, personal data.
・「機密性の侵害」 - 不正又は偶発的な個人データの開示又は個人データへのアクセスが発生した場合
・「完全性の侵害」 - 不正又は偶発的な個人データの変更が発生した場合
・「可用性の侵害」 - 偶発的又は不正な、個人データへのアクセスの喪失 [15] 又は個人データの破壊が発生した場合

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.
また、状況によっては、個人データの機密性、完全性及び可用性の侵害のすべてが同時に関与する場合及びそのいずれかの組み合わせが関与する場合もあり得ることに留意すべきである。

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.
機密性又は完全性の侵害があったか否かの判断は、比較的明白であるが、可用性の侵害があったか否かの判断は、それほど明白ではない。個人データの恒久的な喪失又は破壊が生じた場合、かかる侵害は常に、可用性の侵害であるとみなされる。

---

[14] See Opinion 03/2014
Opinion 03/2014 参照

[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: "The property of being accessible and useable upon demand by an authorized entity." See https://rmf.org/images/4-CNSS-Publications/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
「アクセス」は、基本的に「可用性」の一部であるということが定着している。例として、NIST SP800-53rev4 は、「可用性」を「適宜かつ確実な情報へのアクセス及び情報の使用の確保」と定義している。下記から参照可能：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
また、CNSSI-4009 は、「権限を有する者が要求に応じてアクセス可能かつ使用可能であるという属性」と言及している。https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf.参照のこと。ISO/IEC 27000:2016 もまた、「可用性」を「権限を有する者が要求に応じてアクセス可能かつ使用可能であるという属性」と定義している。：https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Example

事例

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.

データが、偶発的に、若しくは権限を持たない者により削除された場合、又は確実に暗号化されていたデータの復号化キーを喪失した場合が、可用性の喪失の例に挙げられる。管理者が、バックアップ等からデータへのアクセスを復旧できない場合、かかる状況は、可用性の恒久的喪失とみなされる。

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.

可用性の喪失は、例えば、停電やサービス拒否攻撃、個人データの使用不能化等、組織の通常サービスに対し甚大な障害が生じた場合にも生じ得る。

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".

個人データの可用性の一時的喪失は、侵害とみなすべきかという疑問が生じるかもしれない。また、侵害とみなす場合は、誰に通知すべきかが問題となる。GDPR の第 32 条「取扱いの安全性」は、リスクに応じた一定レベルのセキュリティを担保するための技術的かつ組織的対策を実施する場合、とりわけ、「取扱システム及び取扱サービスの現在の機密性、完全性、可用性及び回復性を確保する能力」並びに「物的又は技術的なインシデントが発生した際、適時な態様で、個人データの可用性及びそれに対するアクセスを復旧する能力」を考慮すべきである、と説明している。

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).

よって、一定期間、個人データの使用を不可能にするセキュリティインシデントは、データへのアクセスの欠如が、自然人の権利及び自由に対し重大な影響を与える可能性があるため、侵害の一種と言える。誤解のないように述べるが、計画的なシステムメンテナンスの実行を理由に個人データが利用不能となる場合は、第 4 条(12)に定義する「セキュリティ侵害」ではない。

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.
個人データの恒久的な喪失又は破壊（又はその他一切の種類の侵害）に関して、可用性の一時的喪失が関与する侵害は、第 33 条(5)に従い文書化しておくべきである。かかる措置は、管理者が、かかる文書の閲覧を求める可能性のある監督機関に対し、責任を証明する際に役立つ[16]。しかし、侵害の状況によって、監督機関への通知及び影響を受ける個人への通知が必要な場合と必要でない場合がある。管理者は、個人データの可用性の欠如が自然人の権利及び自由に及ぼす影響の可能性及び深刻度を評価する必要がある。侵害が、個人の権利及び自由に対するリスクに帰結する可能性が低い場合を除き、管理者は、第 33 条に従い通知する必要がある。当然ながら、場合に応じて評価が必要となる。

Examples
事例
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.
病院での事例として、患者に関する重要な医療データが、一時的にでも使用できなくなった場合、手術が延期される、生命が危険にさらされる等、個人の権利及び自由に対するリスクが生じる可能性がある。

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.

[16] See Article 33(5)
第 33 条(5)参照

一方、メディア企業のシステムが、数時間利用不能になり（例：停電による利用不能）、かかる企業が購読者へのニュースレターの送信を妨げられた場合、これにより、個人の権利及び自由に対するリスクが発生する可能性は低い。

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.
管理者のシステムの可用性の喪失は、一時的な喪失の場合もあり、個人に影響を与えない場合もあるが、管理者は、他の理由により通知が必要となる場合もあるため、侵害により生じ得るあらゆる結果を考慮することが重要であることに留意すべきである。

Example
事例
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.
ランサムウェア（身代金が支払われるまで管理者のデータを暗号化する悪意ソフトウェア）による感染は、バックアップによりデータを復旧することが可能であれば、可用性の一時的喪失に帰結する可能性があるが、ネットワークへの侵入が生じ、インシデントが機密性の侵害（つまり、個人データが攻撃者によりアクセスされている）とみなされ、かかる侵害が個人の権利及び自由に対しリスクを及ぼす場合、通知が必要となる場合がある。

3. The possible consequences of a personal data breach
3. 個人データ侵害により起こり得る帰結

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].
侵害は、個人に対し様々な種類の重大な悪影響を与える可能性がある。かかる悪影響は、物理的、有形的又は無形的損害に帰結する可能性がある。GDPR は、かかる帰結には、個人データに対する制御の喪失、個人の権利の制限、差別、身元詐称、詐欺、金銭的損失、仮

[17] See also Recitals 85 and 75
前文第 85 項及び 75 項参照

名化の不正な解除、信用の毀損、守秘義務により保護されている個人データの機密性の喪失が含まれると説明している。また、かかる個人に対するその他の重大な経済的又は社会的不利益も含まれる[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].
よって、GDPR は、発生するであろうかかる悪影響のリスクに帰結する可能性が低い場合を除き、所轄監督機関への侵害の通知を管理者に求めている。かかる悪影響が生じる可能性が高い場合、GDPR は、影響を受ける個人への可及的速やかな侵害の通知を管理者に求めている[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:
侵害の特定、個人に対するリスクの評価及び必要に応じた通知を実施可能にしておくことの重要性については、GDPR の前文第 87 項において強調されている。

> "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."
> 「個人データ侵害が発生したかどうかを迅速に確定するため、そして、監督機関及びデータ主体に対して速やかに連絡するための全ての適切な技術的な保護及び組織上の措置が実装されているか否かが確認されなければならない。特に、その個人データ侵害の性質及び重大性、その結果として生じる事態及びデータ主体に対する悪影響を考慮に入れた上で、不当な遅滞なく通知が行われたという事実が立証されなければならない。そのような通知は、本規則に定める監督機関の職務及び権限に従い、監督機関の介入を招くものとなりうる。」

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.
セクション IV において、個人に対する悪影響のリスク評価に関する指針についてさらに考察する。

[18] See also Recital 86.
前文第 86 項参照

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 (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.

第 33 条及び 34 条の要件が満たされている場合においても、管理者がデータ侵害について、監督機関又はデータ主体のいずれか又は両者への通知を怠った場合、監督機関は、第 58 条(2)に基づく是正措置に伴う又は単独による適切な制裁金 [19] の賦課を含む、あらゆる是正措置をその裁量により考慮する選択肢を提示される。制裁金を科すことを選択した場合、その金額は、最大で 1,000 万ユーロ又は GDPR の第 83 条(4)(a)に基づく全世界における年間総売上高の 2%とすることができる。侵害の通知の懈怠が、既存の安全対策の欠如又は不足を露呈する場合があることに留意しておくことも重要である。制裁金に関する第 29 条作業部会のガイドラインには、「単一の事案にて複数の異なる違反が一度に発生した場合、監督機関が最も深刻な違反の範囲内で効果的、比例的及び抑止的な水準の制裁金を適用することができることを意味している」と記載されている。かかる場合、監督機関は、侵害の通知又は報告（第 33 条及び 34 条）の懈怠に対し制裁を科す一方で、また別の侵害として、安全対策の欠如（不足）（第 32 条）に対しても制裁を科す可能性がある。なぜなら、これらは２つの別の侵害であるからである。

II. Article 33 - Notification to the supervisory authority

II. 第 33 条 - 監督機関への通知

[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
詳細については、制裁金の適用及び設定に関する第 29 条作業部会ガイドラインを参照のこと。下記から参照可：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

A. When to notify

A. 通知すべき場合

1. Article 33 requirements

1. 第 33 条の要件

Article 33(1) provides that:

第 33 条(1)は、下記のとおり定めている。

> "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."
>
> 「個人データ侵害が発生した場合、管理者は、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがない場合を除き、不当な遅滞なく、かつ、それが実施可能なときは、その侵害に気づいた時から遅くとも 72 時間以内に、第 55 条に従って所轄監督機関に対し、その個人データ侵害を通知しなければならない。監督機関に対する通知が 72 時間以内に行われない場合、その通知は、その遅延の理由を付さなければならない。」

Recital 87 states[20]:

前文第 87 項 [20] は、下記のとおり定めている。

> "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."
>
> 「個人データ侵害が発生したかどうかを迅速に確定するため、そして、監督機関及びデータ主体に対して速やかに連絡するための全ての適切な技術的な保護及び組織上の措置が実装されているか否かが確認されなければならない。特に、その個人データ侵害の性質及び重大性、その結果として生じる事態及びデータ主体に対する悪影響を考慮に入れた上で、不当な遅滞なく通知が行われたという事実が立証されなければならない。そのような通知は、本規則に定める監督機関の職務及び権限に従い、監督機関の介入を招くものとなりうる。」

[20] Recital 85 is also important here.
前文第 85 項も重要である。

2. When does a controller become “aware”?

2. 管理者が「認識」した時点とは

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.

上記に詳述したように、GDPR は、侵害が生じた場合は、不当に遅滞することなく、また可能な場合は、かかる侵害を認識した後 72 時間以内に、侵害について通知することを管理者に求めている。これに関し、管理者が侵害を「認識」した時点とは、いつの時点のことを言うのかという疑問が生じる可能性がある。第 29 条作業部会は、管理者が、個人データの侵害に至ったインシデントが生じたことを合理的な程度に確信した時点に「認識」したとみなされるべきであると考慮している。

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 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.

ただし、上述したように、GDPR は、個人データの侵害が生じたか否かを速やかに確証し、監督機関及びデータ主体に迅速に報告するためのあらゆる適切な技術的保護及び組織的対策の実施を管理者に求めている。また、不当に遅滞することなく通知が行われた事実は、特に、個人データ侵害の性質及び重大性並びにその帰結及びデータ主体に対する悪影響を鑑みて確証すべきであるとも述べている[21]。かかる規定は、適切な措置を講じられるように、一切の侵害を適宜確実に「認識」する義務を管理者に科す。

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

[21] See Recital 87
前文第 87 項参照

determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.
正確にどの時点で、管理者が特定の侵害を「認識」したとみなすことができるかは、特定の侵害の状況による。侵害が生じたことが初めから比較的明白である場合もあるが、個人データが侵害されたことを確証するのに時間がかかる場合もある。しかし、ここで重点を置くべきは、個人データが実際に侵害されたか否かを判断するためにインシデントを調査し、侵害されていた場合は、是正措置を講じて必要に応じて通知するための迅速な措置を講じることである。

Examples
事例

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.
1. 暗号化されていない個人データとともにUSBキーを紛失した場合､権限を持たない者が､かかるデータへのアクセスを取得したか否かを確認することは不可能である場合が多いが、管理者が、機密性の侵害が生じたか否か確証できない場合であっても、可用性の侵害が生じていることについては、合理的な程度の確信があるため、かかる状況は通知しなければならない。よって、管理者は、USB キーの紛失に気付いた時点に、侵害を「認識」したとされる。

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".
2. 第三者が、管理者の一顧客の個人データを偶発的に受領したことを管理者に通知し、不正開示の証拠を提出した場合、管理者は、機密性侵害の明白な証拠を提示されているため、侵害を「認識」したことに疑いはない。

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".
3. 管理者が、そのネットワークへの侵入の可能性を検知し、当該システムに保存している個人データが侵害されていないかを確証するために当該システムを確認し、侵害されてい

ることを確認した場合、管理者は、侵害の明白な証拠を取得しているため、侵害を「認識」したことに疑いはない。

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.
4. サイバー犯罪者が、管理者のシステムをハッキングした後に管理者に身代金を要求する為に、連絡した場合、管理者は、そのシステムを調査して、システムが攻撃されたことを確認した後、侵害が生じた明白な証拠を取得しているため、侵害を「認識」したことに疑いはない。

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 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.
管理者は、個人、メディア組織又はその他の情報源から、データ侵害の可能性について第一報を受けた後に、又はセキュリティインシデントを管理者独自に検知した後に、侵害が実際に生じたか否かを確証するために、短期間の調査を行うことができる。かかる調査期間中、管理者は、侵害を「認識」したものとみなされない場合がある。しかしかかる初期調査は、可及的速やかに開始し、侵害が生じたか否かについて合理的な程度の確信を以て確証すべきことが期待される。より詳細な調査は、その後に行うことができる。

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.
管理者は、侵害を認識した後、通知可能な侵害については、不当に遅滞することなく、また可能な場合は、72 時間以内に通知しなければならない。かかる期間中、管理者は、通知要件が発生するか否か、また侵害に対する措置が必要であるか否かを判断するために、個

[22] See WP29 Guidelines on DPIAs here:
DPIA に関する第 29 条作業部会ガイドライン参照：http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

人に対し生じ得るリスクを評価すべきである。しかし管理者は、関連する処理作業を実行する前に行われるデータ保護影響評価（DPIA）[22] の一環として、侵害により生じ得る潜在的リスクについて既に初期評価を行っている場合がある。しかし、DPIA は、何らかの実際の侵害の、特定の状況よりも全体的な状況の評価となる場合がある。よって、いかなる場合においても、かかる特定の状況を考慮した追加評価が必要となる。リスク評価に関する詳細については、セクション IV を参照すること。

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.
大抵の場合において、かかる事前措置は、初回警告後（つまり、管理者又は処理者が、個人データが関与する可能性のあるセキュリティインシデントが生じたことを疑った時点）に速やかに完了すべきである。 - かかる事前措置は、例外的場合のみ、より時間をかけるべきである。

Example
事例
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.
個人が、当該個人による管理者のサービスの（実際の）使用に関する個人データを包含した、管理者を騙る E メールを受信したことを、管理者のセキュリティが侵害されていることを示唆しつつ、管理者に報告する。管理者が、短期間の調査を行い、そのネットワークへの侵入及び個人データへの不正アクセスの証拠を特定する。管理者は、かかる特定時点に、侵害を「認識」したとみなされ、かかる侵害が個人の権利及び自由に対しリスクを及ぼす可能性が低い場合を除き、監督機関への通知が求められる。管理者は、侵害に対する適切な是正措置を講じる必要がある。

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

[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.

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.
よって管理者は、侵害を検知し、それに対処できる組織内プロセスを確立しておくべきである。例として、データ取扱いにおける不規則事象を検知するために、管理者又は処理者は、データフロー及びログのアナライザー等の特定の技術対策を用いることができる。これにより、ログデータと相関させることにより、事象及び警告を検知することが可能になる[23]。侵害が検知された際、かかる侵害に対処できるように適切なレベルの管理職員に上申することに加え、求められる場合は、第 33 条に従い通知し、必要に応じて第 34 条に従い通知することが重要である。かかる対策及び報告のメカニズムは、管理者のインシデント対応計画及び・又は管理取扱書に詳述することができる。かかる措置は、管理者が、侵害管理並びに適切なインシデントの上申方法及び上申の要否について効率的に計画し、組織内の実施責任者を判断する際に役立つ。

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).
管理者は、管理者が使用するすべての処理者と、侵害が発生した場合は処理者自身が管理者に通知する義務を負うという取り決めを交わしておくべきである（下記参照）。

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.
侵害の防止、対応及び対処が可能な適切な対策を確立しておくことは管理者及び処理者の責任であるが、すべての場合において講じるべき実践的な措置が存在する。

- 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.
- すべてのセキュリティ関連事象に関する情報を、インシデントへの対応、侵害の存在の確証及びリスク評価を実施する担当者又はかかる任務を担う者に報告する。

- 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.

データの保管、変更又は消去等の監査能力を支持するログデータも、個々の処理作業を開始した者に関する個人データとみなすことができることに留意すべきである。

・その後、報告を受けた組織の関連部署とともに、侵害に起因する個人に対するリスクを評価する（リスクの有無の可能性、リスクレベルの評価）。

・Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
・監督機関への通知及び必要に応じて影響を受ける個人への侵害の可能性の報告を行う。

・At the same time, the controller should act to contain and recover the breach.
・同時に、管理者は、侵害の阻止及び復旧のための措置を講じる。

・Documentation of the breach should take place as it develops.
・侵害の展開を文書化する。

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.
よって、管理者が、初回警告の時点で対応し、侵害が実際に生じたか否かを確証する義務を負うことは明白である。かかる短期間に一定の調査が可能となり、管理者は、証拠及びその他の関連詳細事項を収集することができる。しかし、管理者が、合理的な程度の確信を以て、侵害が生じたと確証した後、第 33 条(1)の諸条件が満たされている場合、管理者は、不当に遅滞することなく、また可能な場合は 72 時間以内に [24]、監督機関に通知しなければならない。管理者が、適宜措置を講じない場合で、侵害が生じたことが明白になった場合、かかる懈怠は、第 33 条に定める通知の懈怠とみなすことができる。

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 条は、管理者及び処理者が、個人データに対する適切なレベルのセキュリティを担保するために適切な技術的かつ組織的対策を確立しておくべきであることを明白にしている。

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at:
期間、日時及び制約に関し適用される規則を定めた規則 No. 1182/71 参照。下記から閲覧可能：
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN：

侵害を速やかに検知し、対処及び報告する能力は、かかる対策の必須要素とみなすべきである。

3. Joint controllers

3. 共同管理者

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 条は、共同管理者に関係し、共同管理者は、GDPR の遵守に関する各々の責任を定めておくべきであるとしている[25]。これには、第 33 条及び 34 条に基づく義務を遵守する責任を負う当事者を定めておくことが含まれる。第 29 条作業部会は、共同管理者間の契約上の取り決めに、GDPR の侵害通知義務の遵守について主導する又は責任を負うのはどの管理者かを特定する定めを包含すべきと勧告している。

4. Processor obligations

4. 処理者の義務

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".

管理者は、個人データの保護に対し全体的責任を負うが、処理者は、管理者が侵害の通知を含む管理者の義務を遵守できるようにするための重要な役割を有している。実際に、第 28 条(3)は、処理者による取扱いは、契約又はその他の法的措置に準拠するものとすると定めている。第 28 条(3)(f)は、処理者が、「取扱いの性質及び処理者が利用可能な情報を考慮に入れた上で、第 32 条から第 36 条による義務の遵守の確保において、管理者を支援する」ことを、契約又はその他の法的措置により定めるべきであるとしている。

[25] See also Recital 79.
前文第 79 項参照。

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 条(2)は、処理者が管理者により使用される場合で、処理者が、管理者に代わって取り扱っている個人データの侵害を認識した場合、処理者は、「不当に遅滞することなく」管理者に通知しなければならないことを明白にしている。処理者は、侵害について管理者に通知する前に、侵害によりリスクが発生する可能性を最初に評価する必要がないことに留意すべきである。侵害を認識した後に、かかる評価を実施しなければならないのは管理者である。処理者は、侵害が生じたか否かを確証し、管理者に通知する必要があるだけである。管理者は、かかる目的を達成するために処理者を利用する。よって、原則として、管理者は、処理者から侵害について報告を受けた後、侵害を「認識」したものとみなされるべきである。処理者に課される管理者への通知義務により、管理者は、侵害に対処し、第 33 条(1)に従い監督機関に、また第 34 条(1)に従い影響を受ける個人に通知する必要があるか否かを判断することが可能になる。処理者により破壊又は紛失された個人データのコピー又はバックアップが管理者の手元に留まっている場合等、処理者が侵害に関連するすべての事実を認識できる立場にない場合、管理者が、侵害の調査を実施することを望む場合がある。これは、管理者がその後に通知する必要があるか否かに影響を与える場合がある。

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 は、処理者による管理者への警告の期限について、「不当に遅滞することなく」警告しなければならないという定め以外、明白な期限を定めていない。よって、第 29 条作業部会は、侵害について管理者に速やかに通知し、詳細が明らかになるに従い段階的に侵害に

関する追加情報を提供することを処理者に勧告している。かかる措置は、管理者が、72 時間以内に監督機関に通知するという要件を満たすことを可能にするために重要である。

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.
上述したように、管理者と処理者との間の契約において、GDPR のその他の定めに加えて、第 33 条(2)に明記されている要件を満たす方法を特定しておくべきである。これには、管理者による 72 時間以内の監督機関への報告義務をサポートするための、処理者による早期通知要件を包含することができる。

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.
処理者が、同一のインシデントにより影響を受ける複数の管理者にサービスを提供している場合、処理者は、各管理者にインシデントの詳細を報告しなければならない。

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.
管理者が、管理者を代理して通知を行うための適切な権限を処理者に与えており、かかる権限が、管理者及び処理者間の契約上の取り決めの一部である場合、処理者は、管理者を代理して通知を行うことができる。かかる通知は、第 33 条及び 34 条に従い行わなければならない。ただし、通知を行う法的責任は、管理者に留まることに留意することが重要である。

B. Providing information to the supervisory authority
B. 監督機関への報告

1. Information to be provided
1. 提供すべき情報

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:
管理者が監督機関に侵害を通知する場合、第 33 条(3)は、管理者が最低でも下記を実行するよう定めている。

“(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.”
「(a)可能な場合、関連するデータ主体の類型及び概数、並びに、関係する個人データ記録の種類及び概数を含め、個人データ侵害の性質を記述する；
(b)データ保護オフィサーの名前及び連絡先、又は、より多くの情報を入手することのできる他の連絡先を連絡する；
(c)その個人データ侵害の結果として発生する可能性のある事態を記述する；
(d) 適切な場合、起こりうる悪影響を低減させるための措置を含め、その個人データ侵害に対処するために管理者によって講じられた措置又は講ずるように提案された措置を記述する。」

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 は、データ主体又は個人データ記録の分類方法を定義していない。しかし、第 29 条作業部会は、データ主体を分類する際、個人データが侵害により影響を受ける個人の様々な種類を参照することを示唆している。特に、子ども及びその他の弱者、障害者、被雇用者又は顧客等を含む、使用される記述子に応じて分類することができる。同様に、個人データ記録を分類する際は、健康関連データ、教育関連の記録、公的介護情報、財務詳細、銀行口座番号、パスポート番号等、管理者が取り扱う記録の様々な種類を参照することができる。

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.

前文第 85 項は、個人に生じる損害に歯止めをかけることを通知の目的の一つとすることを明確にしている。よって、データ主体の種類又は個人データの種類が、侵害により生じる特定の損害のリスクを示唆する場合（例：身元詐称、詐欺、金銭的損失、守秘義務に対する脅威）、通知において、かかる種類を示唆することが重要である。よって、侵害により生じる可能性のある結果を説明することを要件としているのである。

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.
正確な情報（例：影響を受けるデータ主体の正確な数）が取得できない場合においても、かかる事態が、侵害の適宜通知の障壁となるべきではない。GDPR は、影響を受ける個人の数及び関連する個人データ記録の数を概算することを許可している。正確な数値の提供ではなく、侵害による悪影響への対処に焦点を当てるべきである。

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.
よって、侵害が生じたことが明白になった場合で、侵害の範囲が認識できていない場合、段階的通知（下記参照）は、通知義務を満たすためには安全な方策である。

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 条(3)は、管理者は、「少なくとも」本情報を通知すべきであると定めている。よって、管理者は、必要に応じて、追加の詳細情報を提供することを選択することができる。侵害の種類（機密性、完全性又は可用性）によっては、各事象の状況を完全に説明するための追加情報の提供が必要とされる場合がある。

Example
事例
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.
処理者に侵害の主要因がある場合、特に、かかる侵害が、同一の処理者を利用している複数の他の管理者の個人データレコードに影響するインシデントとなった場合、管理者は、

監督機関への通知の一環として、その処理者の名称を通知することが有益である場合がある。

In any event, the supervisory authority may request further details as part of its investigation into a breach.
いずれにしろ、監督機関は、侵害の調査の一環として、追加の詳細情報を求めることができる。

2. Notification in phases
2. 段階的通知

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:
侵害の性質によっては、インシデントに関連するすべての事実をはっきりさせるために、管理者によるさらなる調査が必要となる場合がある。よって、第 33 条(4)は、下記のように定めている。

"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."
「同時に情報を提供できない場合、その範囲内において、その情報は、更なる不当な遅滞なく、その段階で提供できる。」

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.

つまり、管理者が侵害を認識した後 72 時間以内に、インシデントの完全かつ包括的な詳細情報が、常に取得可能になるわけではないため、GDPR は、管理者が、常にかかる時間内に、侵害に関する必要なすべての情報を取得できるわけではないことを認識している。よって、GDPR は、段階的通知を許可している。これは、侵害の性質及び侵害された個人データの範囲を完全にはっきりさせるためには、詳細な犯罪科学捜査が必要となる可能性のある、ある種のサイバーセキュリティインシデント等、より複雑な侵害が発生した場合により妥当することが多い。よって、多くの場合、管理者は、その後の追加情報を用いて、さらなる調査及びフォローアップを行わなければならなくなる。管理者が、第 33 条(1)に従い情報提供の遅滞の理由を通知する限り、かかる対応は許可される。第 29 条作業部会は、管理者が監督機関に最初に通知する際に、必要なすべての情報を入手していないこと及び詳細情報を後に提供することを監督機関に伝えることを管理者に勧告している。監督機関は、追加情報の提供方法及び提供時期について同意すべきである。かかる同意は、管理者が、監督機関に提供する必要のある、侵害に関連する追加の詳細事項を認識した場合に、同意された提供時期以外のいずれかの後の段階で追加情報を提供することを妨げない。

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.
通知要件は、管理者に、侵害に対し迅速に措置を講じ、侵害を阻止し、可能な場合は、侵害された個人データを復旧し、監督機関に関連する助言を求めることを促すことに焦点を当てている。72 時間以内の監督機関への通知は、管理者が、個人に通知するか否かの判断が正しいかを確認することを可能にする。

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 communicate the breach to the data subject where it is required.
しかし、監督機関への通知の目的は、影響を受ける個人に通知するか否かについての指針を得ることだけではない。侵害の性質及びリスクの深刻度によって、管理者が、影響を受ける個人に遅滞なく通知する必要があることが明白となる場合もある。例として、身元詐

[26] See Article 9.
第 9 条参照

称の喫緊の脅威が存在する場合や、特別な種類の個人データ [26] がオンラインで開示された場合、管理者は、侵害を阻止し、関連する個人に通知するために、不当に遅滞することなく措置を講じるべきである（セクション III 参照）。例外的状況においては、監督機関に通知する前に、影響を受ける個人に通知すべき場合もある。より一般的に述べると、データ主体への侵害通知が必要とされる場合、監督機関への通知は、かかるデータ主体に侵害を通知しない理由にはならない場合がある。

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.
また管理者は、監督機関に初期通知を行った後に、追跡調査により、セキュリティインシデントが阻止され、実際には侵害が生じなかったことの証拠が明らかになった場合、監督機関に対し情報を更新することができることを明白にしておくべきである。かかる情報は、監督機関に既に提供されている情報に追加することができ、インシデントが侵害ではなかったと記録することができる。最終的に侵害ではないことが明らかになったインシデントを報告したことに対する罰則はない。

Example
事例
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.
管理者が、その顧客の個人データのコピーを包含する USB キーを紛失したことを、侵害を検知した後 72 時間以内に監督機関に通知したが、その後に、USB キーは管理者の敷地内の別の場所に保管されていたことが分かり復旧された場合、管理者は、監督機関に対し、情報を更新し、通知の修正を要求する。

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.
段階的通知のアプローチは、指令 2002/58/EC、規則 611/2013 及びその他のインシデント自己報告の既存の義務に基づき、既に取り入れられていることに留意すべきである。

3. Delayed notifications
3. 通知の遅滞

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 条(1)は、72 時間以内に監督機関への通知が行われない場合、遅滞の理由を付すべきことを明白にしている。かかる規定は、段階的通知の概念に加えて、管理者が、常にかかる期間内に侵害を通知できるわけではないこと、及び通知の遅滞が許される場合があることを認めている。

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.
かかる事態は、例として、短期間に、複数の同様の機密性の侵害が管理者に生じ、同一の方法により多数のデータ主体に影響を与えた場合に生じる場合がある。管理者が、侵害を認識し、調査を開始したところ、通知を行う前に、異なる原因の同様の侵害をさらに検知する場合がある。状況によっては、管理者が侵害の範囲をはっきりさせるのに時間がかかり、管理者は、各侵害を個別に通知する代わりに、原因が異なり得る複数の非常に類似した侵害を示した有意義な通知にまとめる。このようにすると、監督機関への通知に、管理者が最初にかかる侵害を認識してから 72 時間以上を要することになる場合がある。

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.
厳密に言えば、個々の侵害は、報告可能なインシデントであるが、管理者は、過剰な負担を避けるために、比較的短期間における同一の方法による同種の個人データの侵害に関する通知であることを前提として、かかるすべての侵害を「まとめて」通知することができる。多様な方法による多種類の個人データが関連する一連の侵害が生じた場合、通知は、第 33 条に従い、各侵害を報告する通常の方法で行うべきである。

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.
GDPR は、一定範囲の通知の遅滞を許可しているが、常に許可されるものであるとみなすべきではない。72 時間以内に複数の同様の侵害を報告する場合にも、まとめて通知することができることを指摘しておく。

C. Cross-border breaches and breaches at non-EU establishments
C. 越境侵害及び EU 外拠点における侵害

1. Cross-border breaches
1. 越境侵害

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:
個人データの越境取扱い [27] が行われる場合、侵害が複数の加盟国におけるデータ主体に影響を及ぼすことがありうる。第 33 条(1)は、侵害が生じた場合には、管理者は GDPR 第 55 条 [28] に従って権限ある監督機関に通知すべき旨を明らかにしている。第 55 条(1)は次のように述べている：

> "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."
> 「各監督機関は、その監督機関の加盟国の領土上において、本規則に従って割り当てられる職務を遂行し、かつ、付与された権限を行使するための職務権限をもつものとする。」

However, Article 56(1) states:
但し第 56 条(1)は次のように述べている：

> "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)
第 4(23)条参照
[28] See also Recital 122.
前文第 122 項も参照

「第 55 条を妨げることなく、管理者又は処理者の主たる拠点又は単一の拠点の監督機関は、第 60 条に定める手続に従い、その管理者又は処理者によって行われる越境取扱いに関し、主監督機関として行動するための職務権限をもつものとする。」

Furthermore, Article 56(6) states:
さらに第 56 条(6)は次のように述べている：

"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."
「主監督機関は、当該管理者又は処理者によって行われる越境取扱いについて、その管理者又は処理者の単独の担当窓口となる。」

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.
このことは、越境取扱いの文脈において侵害が生じて通知が必要な場合はいつでも、管理者は主監督機関に通知する必要があるということを意味する [29]。従って、侵害対応計画の策定にあたっては、管理者は、どの監督機関が自らが通知するべき主監督機関なのかについて、確認しなければならない [30]。これにより管理者は、第 33 条に関する侵害に迅速に対応しそれに関する義務を充足することができるようになる。越境取扱いを含む侵害が生じた場合、通知は主監督機関に行わなければならないが、その機関は必ずしも影響を受けるデータ主体が存在する場所やまさに侵害が起こった場所とは限らないということを明らかにするものとする。主監督機関に通知するにあたっては、管理者は場合に応じて、その侵害が他の加盟国に所在する拠点を含んでいるか、またどの加盟国でデータ主体がその侵害に

[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
管理者又は処理者の主監督機関の特定についての第 29 条作業部会ガイドライン参照。以下 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
欧州諸国データ保護期間全般の連絡先詳細リスト参照。以下: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

より影響を受ける可能性があるかについて明示するものとする。管理者が、主監督機関をどのように特定するか疑問がある場合は、最低限、その侵害が生じた現地の監督機関に通知するものとする。

2. Breaches at non-EU establishments

2. 非 EU 拠点における侵害

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 条は、GDPR の領域の範囲に関係し、EU 内で設立されたものでない管理者又は処理者による個人データの取扱いに適用される場合も含む。とりわけ第 3 条(2)は次のように述べている[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:
> 「取扱活動が以下と関連する場合、本規則は、EU 域内に拠点のない管理者又は処理者による EU 域内のデータ主体の個人データの取扱いに適用される：
> (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
> (a) データ主体の支払いが要求されるか否かを問わず、EU 域内のデータ主体に対する物品又はサービスの提供。又は
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."
> (b) データ主体の行動が EU 域内で行われるものである限り、その行動の監視。」

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

第 3 条(3)もこれに関連しており、次のように述べている[32]:

> "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."
> 「本規則は、EU 域内に拠点のない管理者によるものであっても、国際公法の効力により加盟国の国内法の適用のある場所において行われる個人データの取扱いに適用される。」

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

[31] See also Recitals 23 and 24
前文第 23、24 項も参照
[32] See also Recital 25
前文第 25 項も参照

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).
従って、EU 内に拠点のない管理者が、第 3 条(2)又は第 3 条(3)の対象で、なおかつ侵害が生じた場合も、この管理者はやはり第 33 条及び 34 条に基づく通知義務に拘束される。第 27 条は、管理者(及び処理者)が、第 3 条(2)が適用される場合に、EU 内に代理人を任命することを求めている。このような場合、第 29 条作業部会は、管理者の EU 内の代理人が設定された加盟国における監督機関に通知を行うことを推奨している [33]。同様に、処理者が第 3 条(2)の対象である場合、処理者の義務、とりわけここで関連する、第 33 条(2)に基づき管理者に侵害を通知する義務に拘束される。

D. Conditions where notification is not required
D. 通知を要しない場合の条件

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 条(1)は、「自然人の権利及び自由に対するリスクを発生させるおそれがない」侵害は、監督機関への通知を要しないことを明らかにしている。例えば、個人データが既に公に利用可能で、当該データの開示が個人に危険を及ぼすおそれとならない場合が挙げられる。これは、関連する侵害すべてを所轄官庁に通知しなければならないとする、指令 2009/136/EC における公的に利用可能な電子通信サービスのプロバイダーについての現存の侵害通知要件とは対照的である。

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

[33] See Recital 80 and Article 27
前文第 80 項及び第 27 条参照
[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
第 29 条作業部会, 侵害通知についての意見 03/2014
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

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.
侵害通知についての 2014 年 3 月意見書において [34]、第 29 条作業部会は、先端技術のアルゴリズムで暗号化された個人データの秘密保持侵害は依然として個人データについての侵害であって通知を要すると説明した。但し、キーの秘密性が損なわれていない場合、－すなわちキーがセキュリティ侵害によって漏えいされておらず、アクセス権限のない者が利用可能な技術的手段によって突き止められないように作成されていた場合－データは原則として理解できないものである。従って、侵害が個人に悪影響を与えるおそれはなく、よってこれらの個人に対する連絡は不要である [35]。但し、データが暗号化されていても、管理者が適切なバックアップを有していなければ、喪失や改変によりデータ主体に悪影響を及ぼすことがありうる。この場合、データ自体が適切な暗号化措置の対象になっていたとしても、データ主体に対する連絡が必要である。

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.
第 29 条作業部会はまた、パスワードのような個人データが安全にハッシュ化されソルト付与されていて、ハッシュ化した数値が先端技術の暗号キーハッシュ関数で計算され、そのデータをハッシュ化するのに用いるキーが侵害によって漏えいされておらず、なおかつそのデータをハッシュ化するのに用いるキーが、アクセス権限のない者が利用可能な技術的手段によって確認できない方法で生成されている場合にもあてはまる旨を定めている。

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

[35] See also Article 4(1) and (2) of Regulation 611/2013.
規制 611/2013 の第 4 条(1)及び(2)も参照。

よって、個人データが無権限な者にとっては本質的に理解不可能なものとされて、そのデータがコピーであるかバックアップが存在する場合は、適切に暗号化された個人データを含む秘密の侵害を監督機関に通知する必要はないと言える。これは、そのような違反は個人の権利と自由をリスクにさらすおそれがないからである。このことは当然ながら、高いリスクがないと思われることからその個人にも通知をする必要がないことを意味する。ただし、個人の権利と自由に対するリスクのおそれがない場合には当初は通知が必要とされないとしても、時の経過と共に事態が変わり、リスクを再評価する必要がありうることは念頭におくべきである。例えば、後にキーが漏えいしたことが判明した場合、又は暗号ソフトウェアの脆弱性が露わになった場合は、やはり通知は必要となりうる。

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".

さらに、暗号化された個人データのバックアップが無いところに侵害が生じた場合、利用可能性についての侵害が生じることとなり、これは個人をリスクにさらすことになりうることから、通知が必要となりうる。同様に、個人データのバックアップが存在するとしても、侵害が暗号化されたデータの喪失を含む形で生じた場合、そのバックアップからのデータの回復に要した時間の長さと、その利用可能性の欠如が個人に及ぼす影響によっては、これもなお報告対象の侵害となりうる。第 32 条(1)(c)が述べる通り、セキュリティの重要な要因は「物的又は技術的なインシデントが発生した際、適時な態様で、個人データの可用性及びそれに対するアクセスを復旧する能力」である。

Example

事例

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.

監督機関への通知を要しない侵害は、管理者及びそのスタッフが使用する、安全に暗号化されたモバイルデバイスの喪失である。暗号キーが依然として管理者の安全な保持下にあり、これが個人データの唯一のコピーでない限りは、個人データは攻撃者にとってアクセス不能である。このことは、侵害が問題になっているデータ主体の権利及び自由へのリスクを生じさせるおそれがないことを意味する。暗号化キーが漏えいした又は暗号化のソフトウェア若しくはアルゴリズムが脆弱であることが後に判明した場合は、自然人の権利及び自由へのリスクは変動し、よって通知が必要となることがある。

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.

ただし、データが実際には安全に暗号化されていなかった状況において、管理者が監督機関に通知しない場合は、第 33 条の不遵守が生じることになる。よって、暗号化ソフトウェアを選択するにあたっては、管理者は、提案された暗号化の品質と適切な実施を入念に検討して、それが実際に提供する保護の水準と、表れたリスクにとってこれが適切か否かを理解するべきである。管理者はまた、その暗号化製品がどのように機能するかの仕様を熟知するべきである。例えば、あるデバイスはスイッチオフされた場合に暗号化されうるが、スタンバイモードの場合にはそうではない。暗号化を使用する一部の製品は、有効化するには各顧客が変更する必要のある「デフォルトキー」を有する。また、暗号化は、現在、セキュリティの専門家によって適切だと判断されていても、数年内に時代遅れになりえるものとも考えられており、これは、データがその製品によって十分に暗号化され、適切な水準の保護が提供されているか否かについて疑問の余地があることを意味する。

III. Article 34 – Communication to the data subject
III. 第 34 条 – データ主体への連絡

A. Informing individuals
A. 個人への通知

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.
一定の場合に、監督機関への通知と並んで、管理者は侵害について、影響を受ける個人に連絡することも必要である。

Article 34(1) states:
第 34 条(1)は次のように述べている:

> "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."
> 「個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、管理者は、そのデータ主体に対し、不当な遅滞なく、その個人データ侵害を連絡しなければならない。」

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.
管理者は、侵害の結果として個人の権利及び自由へのリスクのおそれがない場合を除き、監督機関への通知が必須であることを想起すべきである。さらに、侵害の結果として個人の権利及び自由への高度なリスクのおそれがある場合はその個人にも通知しなければならない。従って、侵害を個人に連絡するか否かの境界線は、監督機関に通知する場合よりも高度であり、すべての侵害が個人への連絡を要するわけではないことから、不要な通知の煩雑さからは免れるようになっている。

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 は、個人への侵害の連絡は「不当な遅延なく」行うものと述べるが、これは可能な限り早くということを意味する。個人への通知の主たる目的は、その個人が自らを保護するために取るべき手段について具体的な情報を提供することである[36]。上記の通り、侵害の性

[36] See also Recital 86.
前文第 86 項も参照

質及びさらされるリスクに応じて、適時の連絡は、個人が、侵害の悪影響から自らを保護するための手段を取るのを助けることになる。

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.
ガイドラインの別紙 B は、侵害が個人へ高度なリスクを生じさせる可能性があり、それにより管理者が影響を受ける者に対して侵害の通知を要する事例の、非網羅的なリストを示す。

B. Information to be provided
B. 提供すべき情報

When notifying individuals, Article 34(2) specifies that:
個人に通知するにあたり、第 34 条(2)は次のように述べている：

> "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)."
> 「本条第 1 項で定める示すデータ主体に対する連絡は、明確かつ平易な言語でその個人データ侵害の性質を記述し、かつ、少なくとも、第 33 条第 3 項(b)、(c)及び(d)に規定された情報及び勧告を含める。」

According to this provision, the controller should at least provide the following information:
この規定に従って、管理者は最低でも以下の情報を提供するものとする：

・a description of the nature of the breach;
・その侵害の性質の記述

・the name and contact details of the data protection officer or other contact point;
・データ保護オフィサー又はその他の連絡窓口の名前及び連絡先

・a description of the likely consequences of the breach; and
・侵害の結果として発生する可能性のある事態の記述、及び

・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.
・侵害に対処するために管理者によって講じられた、又は講ずるように提案された措置の記述。適切な場合、その起こりうる悪影響を低減させるための措置を含む。

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.
侵害に対処しその起こりうる悪影響を低減させるために講じられる措置の例として、関連する監督機関にその侵害を通知した後に、管理者が侵害を制御してその影響を削減するための助言を受けた旨を管理者は述べることができる。管理者はまた、適切な場合、侵害により発生する可能性のある悪影響から個人が自らを守るための具体的な助言(例えばアクセスの認証情報が漏えいした場合のパスワードの変更)を提供するべきである。ここでもまた、管理者は、ここで必要とされるもの以上の情報を提供することを選択できる。

C. Contacting individuals
C. 個人への接触

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).
原則として、関係する侵害は、過大な負担を要する場合を除き、影響を受けるデータ主体に対して直接連絡されるべきである。連絡に過大な負担を要する場合、データ主体が平等に効果的な態様で通知されるような広報又はそれに類する方法に変更される(第 34 条(3)c)。

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.
侵害をデータ主体に連絡するにあたっては、専らそれだけに限定した告知をするものとし、例えば定期的なアップデート、ニュースレター又は通常の告知のようなその他の情報とあわせて発信してはならない。このことにより、侵害についての連絡が明確でわかりやすくなる。

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.
わかりやすい連絡手段の例としては、直接的な告知(例：電子メール、SMS、ダイレクトメッセージ)、人目を引くウェブサイトバナー又は通知、郵送、及び印刷媒体での人目を引く広告を含む。プレスリリース又は会社ブログ内のみに限定された通知は、侵害を個人に連絡する実効性のある手段ではない。第 29 条作業部会は、管理者が影響を受ける個人全員に対して情報を適切に連絡する機会を最大化する手段を選択するよう勧告する。状況に応じて、これは、管理者が、単一の連絡経路を使用するのではなく、複数の連絡手段を採用することを意味することがある。

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.
管理者はまた、個人が自らに提供される情報を確実に理解できるようにするため、適切な代替的形式及び適宜の言語で、その連絡へのアクセスを確保できるようにする必要がある。例えば、個人に侵害を連絡するにあたっては、受信者との通常の業務の過程であらかじめ使用した言語が一般的には適切であろう。しかしながら、その侵害が、あらかじめ管理者が接触したことがなかったデータ主体や、特に管理者の拠点とする国とは異なった加盟国又はその他の非 EU 加盟国に居住するデータ主体に影響を与える場合は、必要とされるリソースを考慮したうえで、現地国の言語での連絡が望ましいことがある。肝要なことは、データ主体が侵害の性質及び自らを保護するために取りうる手段の理解を手助けすることである。

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.
管理者は、個人への侵害を連絡するための最も適切な連絡経路を最も良く判断できる立場にある(とりわけ、頻繁に自らの顧客と接触する場合)。しかしながら、侵害によって連絡経路が害された場合は、この連絡経路は攻撃者が管理者になりすまして利用することもできるため、管理者はこの連絡経路を使用することには厳に慎重になるべきである。

At the same time, Recital 86 explains that:
同様に、前文第 86 項は次のように述べている：

> "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."
> 「そのようなデータ主体に対する連絡は、監督機関から提供されたガイダンス又は法執行機関のような監督機関以外の関連機関から提供されたガイダンスを尊重しつつ、可能な限り速やかに合理的に実現できるように、かつ、監督機関と密接に協力して、行われなければならない。例えば、損害発生の緊急のリスクを低減させる必要性があることは、データ主体への連絡を督促することになるが、他方、個人データ侵害の継続又は類似の侵害の発生に対抗するための適切な措置の実施の必要性があることは、さらに連絡する時間がかかることを正当化しうる。」

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.
よって、管理者は、第 34 条に従って侵害についてデータ主体に通知することについてのみならず、その個人に送信すべき適切なメッセージ、さらにその個人と接触する最も適切な方法についても助言を求めるべく、監督機関に接触し協議することを望むことがありうる。

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.
これに関連するのが、前文第 88 項に記載した、侵害の通知は「早い段階における開示が個人データ侵害の状況に関する捜査を不必要に妨げてしまう場合、法執行機関の正当な利益を考慮」すべきである、という助言である。このことは、一定の状況においては、正当な理由がある場合に、法執行機関の助言に基づき、管理者はその侵害を影響を受ける個人に連絡することを、その調査が妨げられなくなるまでは遅らせることができることを意味しえる。ただし、それでもなおデータ主体は、その後には直ちに連絡を受ける必要がある。

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).
保持しているデータが個人に連絡するには不十分であったために、管理者が個人に対して侵害を連絡することができない場合であれば、その具体的な状況に応じて、管理者は、合理的に実施可能になり次第すぐにその個人に連絡するべきである(例：個人が、個人データにアクセスするため第 15 条の権利を行使して、管理者に、連絡のための必要な追加情報を提供する場合)。

D. Conditions where communication is not required
D. 連絡を要しない条件

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 条(3)は、侵害があった場合、充足されれば個人に通知を必要としない三条件について記載している。これらは：

・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.
・管理者が、侵害より前に、個人データを保護するための適切な技術上及び組織上の措置、とりわけ、データに対するアクセスが承認されていない者にはその個人データを識別できないようにする措置を適用していた場合。これは、例えば、先端的技術による暗号、又はトークン化を用いた個人データの保護を含みうる。

・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.
・侵害の後直ちに、管理者が、個人の権利及び自由に対する高いリスクがもはや具体化しないようにすることを確保する手段を取っていた場合。例えば、事案の状況に応じて、管理者が、個人データにアクセスした者が何かそれについて行うことができるようになる前に、その者を直ちに特定して対抗措置を取っていた場合。ここでもまた関連するデ

ータの性質に応じて、機密性が侵害されたことによる潜在的な結果に対しては、適切な注意がなお必要である。

・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.
・連絡先が侵害の結果喪失したか、そもそも知らない場合、個人に接触するために過大な負担を必要とすることになる[37]。例えば、統計当局の倉庫が洪水に見舞われて、個人データを含んだ文書が紙形式でのみ保管されていた場合。この場合は、個人が平等に効果的な態様で通知を受けられるように、管理者は広報を行うか、それに類する方法を取らねばならない。過大な負担となる場合、侵害についての情報(侵害により影響を受けた可能性があるものの、管理者が他の手段で接触できない個人にとって有用であることがわかったもの)を要求に応じて利用できる技術的な対応も想定できる。

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.
アカウンタビリティ原則に従って、管理者は、監督機関に対して、これらの条件の 1 つ以上の条件を充足したことを証明できるようにする必要がある[38]。自然人の権利及び自由に対するリスクがない場合には、通知はまずは必要ではないとしても、時の経過と共に事態が変わり、リスクの再評価を要するようになることがありうることは念頭に置く必要がある。

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 employing its available powers and sanctions.

---

[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
過大な負担の問題を検討している、透明性についての第 29 条作業部会ガイドライン参照。以下 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] See Article 5(2)
第 5(2)条参照

管理者が個人に侵害を連絡しないという判断をした場合でも、第 34 条(4)は、監督当局が、その侵害が個人に対する高いリスクを生じさせるおそれがあると判断した場合に、その連絡を求めることがありうる旨を説明している。一方、監督機関は、個人への通知が必要とされない第 34 条(3)の条件が充足される場合も考慮することができる。監督機関が、データ主体に通知しないという判断の根拠が不十分だと判断した場合は、利用可能な権能と制裁を検討することができる。

IV. Assessing risk and high risk
IV. リスク及び高度なリスクの評価

A. Risk as a trigger for notification
A. 通知の要件となるリスク

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:
GDPR は侵害につき通知する義務を導入しているものの、すべての状況において通知することを求めているわけではない：

・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.
・侵害が個人の権利及び自由へのリスクを生じるおそれがない場合を除き、所轄監督機関への通知が要求される。

・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.
・侵害が個人の権利及び自由に高度なリスクを生じるおそれがある場合にのみ、その個人への侵害の連絡が要求される。

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.
このことは、侵害を知った時に直ちに、管理者が侵害の阻止を追求するだけでなく、その侵害から生じうるリスクを評価することが必要であるということが極めて重要だということを意味する。これは 2 つの重要な理由がある。第一に、蓋然性と、個人に対する影響の潜在的重大性を知ることで、管理者はその侵害を阻止し対処する実効的手段を取ることが

できるようになる。第二に、監督機関に対する通知、及び、必要であれば関係する個人に対する通知が必要か否かの判断ができるようになる。

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].
上記で説明したとおり、侵害の通知は、個人の権利及び自由へのリスクを生じるおそれがない場合を除き必要であり、データ主体への侵害の連絡を必要とさせる要件は、個人の権利及び自由への*高度な*リスクを生じるおそれがあるかどうかである。このリスクは、ある個人のデータが侵害された場合に、その個人にとって、身体的、物質的若しくは非物質的な損害につながりうる場合に存在する。このような損害の例は、差別、身元詐称若しくは詐欺、金銭的損失及びレピュテーションへの損害である。侵害が、人種若しくは民族的出自、政治的意見、信教若しくは思想上の信条、又は労働組合の加入を明らかにする個人データを含む場合、又は、遺伝子データ、健康と関連するデータ若しくは性的生活と関連するデータ、又は有罪判決及び犯罪行為、また関連する保護措置と関係するデータを含む場合には、これらの損害が生じる可能性が高い[39]。

B. Factors to consider when assessing risk
B. リスク評価にあたって考慮する要因

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 の前文第 75 項及び第 76 項は、一般的に、リスク評価にあたって、データ主体の権利及び自由に対するリスクのおそれと重大性の両方を考慮すべきことを示唆している。さらに、リスクは客観的評価に基づいて評価すべきことも述べている。

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

[39] See Recital 75 and Recital 85.
前文第 75 項及び前文第 85 項参照。
[40] See WP Guidelines on DPIAs here:
DPIA に関する WP ガイドライン参照：

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.
侵害の結果としての人々の権利及び自由に対するリスクを評価する場合、DPIA で考慮されるリスクとは異なる焦点を有することに留意を要する）[40]。DPIA は、計画とおりデータ取扱を行う際のリスクと、侵害がなされた場合のリスクの両方を考慮する。潜在的な侵害を考慮するに当たっては、一般的な意味でこれが発生するおそれと、結果として起こりうるデータ主体に対する損害を検討する。言い換えれば、仮定的な事象の評価なのである。実際に侵害が生じた場合は、事象は既に起こってしまっているので、侵害の個人に及ぼす影響から生じるリスクに完全に焦点を当てることになる。

Example
事例
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 は、個人データを保護する特定のセキュリティソフトウェア製品の使用の提案は、それがなければ取扱いが個人に及ぼすことになるリスクに対して適切な水準のセキュリティを確保することに適した手段であることを示唆する。しかしながらその後に脆弱性を認識した場合は、保護対象の個人データに対するリスクを阻止することについてのそのソフトウェアの適切性を変質させるものであり、継続中の DPIA の一部として再評価を受ける必要があろう。

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.
製品における脆弱性は後になって利用され、侵害が発生する。管理者は、侵害の具体的状況、影響を受けるデータ、及び個人への影響の潜在的レベル、並びにそのリスクが実現する可能性の程度について評価するものとする。

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

http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]:
従って、侵害の結果としての個人に対するリスクを評価するに当たっては、管理者は、想定される影響の重大性及びその発生の可能性を含む、侵害の具体的状況を考慮するものとする。よって、第 29 条作業部会は、評価が以下の基準を考慮に入れるよう勧告する [41]:

・The type of breach
・侵害の種類

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.
発生した侵害の種類が、個人に対するリスクの水準に影響することがある。例えば、医療情報が無権限の者に開示された秘密侵害は、ある個人の医療情報の詳細が喪失し、利用不能となったという侵害とは異なる結果を個人にもたらしうるのである。

・The nature, sensitivity, and volume of personal data
・個人データの性質、機微性及び量

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.
当然、リスク評価に当たって、主要な要因はその侵害により害された個人データの種類及び機微性である。通常は、データの機微性が高まるほど、影響された人々に害が及ぶリスクも高まるが、データ主体について既に利用可能となっている可能性のある他の個人データについても考慮が必要である。例えば、通常の状況においては個人の氏名及び住所を開示することは、重大な損害を生じる可能性は低い。しかしながら、養父母の氏名及び住所

[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
規制 611/2013 の第 3 条 2 は、電子通信サービス分野における侵害についての通知に関して考慮すべき要因のガイダンスを定めており、これは GDPR に基づく通知の文脈でも有用である。以下参照。 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

が産みの両親に開示された場合は、養父母及び子どもの両方にとって重大な結果が生じうる。

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.
健康データ、身分証明文書、又はクレジットカード明細のような財務情報を含んだ侵害は、すべてそれ自体でも害を生じうるが、併せて使用された場合は、身元詐称のために使用されうる。個人データの組み合わせは、典型的にいえば、単一の断片的な個人データよりも機微性が高い。

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.
ある種類の個人データは、当初は比較的に無害のように見えることがあるが、影響される個人についてそのデータが何を明らかにすることがあるかについては入念な考慮を要する。通常の配達を受ける顧客のリストは特段の機微性はないかも知れないが、休日には配達を停止するよう求めた顧客についての同じデータは、犯罪者にとって有用になるだろう。

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.
同様に、高度に機微性のある個人データは少量でも個人に対して高度な影響を及ぼしうるし、広範囲にわたる詳細情報ならば、その個人についてより広い範囲の情報を明らかにすることがありうる。また、多数のデータ主体についての大量の個人データに影響する侵害は、それに対応して多数の個人に影響を及ぼしうる。

・Ease of identification of individuals
・個人の特定の容易性

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.
考慮すべき重要な要因は、不正アクセスされた個人データにアクセスした者にとって、特定の個人の身元を特定したり、個人の身元を特定するため他の情報とそのデータを照合するのがどの程度容易か、ということである。状況によっては、個人の身元を見いだすために必要な特殊な調査もなしで、侵害された個人データから直接身元特定をすることが可能な場合もある。または、個人データを特定個人と照合するのが極めて困難な場合もありうるが、これも一定の条件下ではやはり可能なことがある。身元特定は、侵害されたデータから直接若しくは間接に可能でありうるが、また、侵害の特定の文脈と、関連する個人の詳細情報についての公の入手可能性にも依存する。これは機密性及び可能性の侵害についてはさらに関係する。

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.
上記のとおり、適切な暗号化レベルにより保護された個人データは、暗号キーを持たない無権限の者にとっては判別不能であろう。さらに、適切に実施された仮名化（第 4 条(5)で「追加的な情報が分離して保管されており、かつ、その個人データが識別された自然人又は識別可能な自然人に属することを示さないことを確保するための技術上及び組織上の措置の下にあることを条件として、その追加的な情報の利用なしには、その個人データが特定のデータ主体に属することを示すことができないようにする態様で行われる個人データの取扱い」と定義される）もまた、個人が侵害の結果として身元特定されるおそれを低減することができる。ただし仮名化技術だけでは、データを判別不能とするものとして扱うことはできない。

・Severity of consequences for individuals.
・個人にとっての結果の重大性

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.
侵害に巻き込まれた個人データの性質に応じて（例えば特殊なカテゴリーのデータ）、生じうる個人への潜在的な損害は非常に重大となりうる。とりわけ、侵害が身元詐称や詐欺、物理的損害、心理的打撃、侮辱又はレピュテーションへの損害を生じうる場合はそうである。侵害が脆弱な個人についての個人データに関連する場合は、これらの個人はより大きな危害のリスクにさらされうる。

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).
個人情報が、意図不明又は悪意を持っている可能性のある者の手にあることを管理者が知っているか否かは、潜在的リスクの水準について影響を及ぼしうる。個人データが、第 4 条(10)で定義するように、第三者、又はその他の取得者に誤って開示される機密性の侵害がありうる。これは、例えば、個人データが、組織の誤った部門、又は通常使用されるサプライヤーの組織に誤って送付された場合に起こりうる。管理者は、取得者に対して、受領したデータを返却するか安全に破棄するか求めることができる。いずれの場合でも、管理者がそれらの相手と継続的な関係を有するとすれば、またそれらの手順、経歴及びその他の関連詳細情報を知っているとすれば、取得者は「信用できる」と考えられる。言い換えれば、管理者は、取得者について一定の確証を有しており、その取得者が誤って送付されたデータを読んだりアクセスしたりしないこと、また、返却の指示を遵守することが合理的に期待できる。データがアクセスされた場合でも、管理者はなお、取得者がそれについ

てさらなる行為をすることなく、直ちに管理者にデータを返却してその回復に協力することを信頼することが可能である。このような場合、管理者が、侵害の後で行うリスク評価に、要因として組み込むことができる － 取得者が信頼されているという事実は、侵害の結果の重大性を無くすことはありうるが、侵害が発生しなかったことを意味するわけではない。但し、このことは、個人に対するリスクのおそれを除去しうるものであり、監督機関又は影響される個人に対して通知することは必要なくなる。重ねて、これはケースバイケースである。それにもかかわらず、管理者はなお、侵害の記録を保持する一般的義務の一部として、その侵害に関する情報を保管しなければならない（下記 V 節を参照）。

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.
個人にとっての結果の永続性も考慮するべきである。これについては、作用が長期間であれば影響もより大きいと考えることができる。

・Special characteristics of the individual
・個人の特別な特性

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.
侵害は、子ども又はその他の脆弱な個人に関する個人データにも影響しうるが、これらの者は、結果としてより大きな危険のリスクにさらされうる。侵害の影響の水準に影響しうる個人に関するその他の要因もありうる。

・Special characteristics of the data controller
・データ管理者の特別な特性

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.
管理者の性質及び役割、並びにその活動は、侵害の結果としての個人に対するリスクの水準に影響しうる。例えば医療機関は、個人データの特殊なカテゴリーのものを取り扱うが、これは、これらの個人データが侵害されれば、新聞の郵送リストに比べると、個人にとってより大きな脅威となることを意味する。

・The number of affected individuals
・影響される個人の人数

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.
侵害は、1 名や数名のみ、又は数千名(それ以上ではないとして)に影響することがある。一般には、影響される個人の数が多いほど、侵害の影響も大きくなりうる。但し、個人データの性質と、それが侵害された文脈次第では、侵害は 1 名の個人についてでも重大な影響を有することがある。ここでもまた、肝要なのは、これらの影響される人々に対する影響の可能性と重大性を考慮することである。

・General points
・一般的な点

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.
したがって、侵害から生じうるリスクの評価に当たっては、管理者は、個人の権利と自由についての潜在的な影響の重大性と、それが発生する可能性の組み合わせを考慮すべきである。明らかに、侵害の結果がより重大であれば、リスクはより高くなるし、同様に、これらのことが生じる可能性が高ければ、リスクはまた高くなる。疑わしい場合は、管理者は、注意の払い過ぎとなってでも通知をするべきである。別紙 B は、個人に対するリスク又は高度なリスクを含む異なった種類の侵害の有用な例を示している。

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].
ネットワーク及び情報の安全についての欧州連合機関(ENISA)は、侵害の重大性の評価方法についての勧告を作成しており、これは、管理者及び処理者が、その侵害管理対応計画の策定にあたって有用と感じるであろう[42]。

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity
ENISA、個人データ侵害の重大性評価方法についての勧告、
https://www.enisa.europa.eu/publications/dbn-severity

V. Accountability and record keeping
V. アカウンタビリティ及び文書保管

A. Documenting breaches
A. 違反の記録

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:
侵害を監督機関に通知する必要があるか否かにかかわらず、管理者は、第 33 条(5)が説明するとおり、すべての侵害についての文書を保管しなければならない：

> "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."
> 「管理者は、その個人データ侵害と関連する事実関係、その影響及び講じられた救済措置を含め、全ての個人データ侵害を文書化しなければならない。その文書は、本条の遵守を検証するために、監督機関が利用できるものとしなければならない。」

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].
これは第 5 条(2)に含まれる GDPR のアカウンタビリティ原則に関連する。通知対象の侵害のみならず通知の対象とならない侵害を記録する目的は、管理者の第 24 条に基づく義務にも関連しており、監督機関はこれらの記録の閲覧を要求できる。従って管理者は、通知の要否を問わず、侵害について内部的な登録を定めることが推奨される [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.

[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.
管理者は、第 30 条に従って保管する自らの取扱活動の記録の一部として侵害を文書化することを選ぶことができる。独立して登録することは必要ではないが、ただしその侵害に関連する情報が明確に特定されて、要求があり次第抽出できることが前提である。

侵害を文書化する際に使う方法及び構成を判断するのは管理者の役割ではあるものの、記録対象の情報については、すべての場合において含むべき主要な要素がある。第 33 条(5)で求められるように、管理者は侵害に関する詳細情報を記録することを要し、その記録にはその原因、発生した事態及び影響された個人データを含むものとする。さらに記録には、侵害の影響及び結果、並びに管理者がとった是正措置も含むものとする。

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 はこれらの文書の保存期間を定めていない。これらの記録が個人データを含む場合は、個人データの取扱いに関する原則に従って適切な保存期間を判断し[44]、取扱いについての法的基準を遵守する[45]のは、管理者の責務である。第 33 条(5)、又はより一般的なアカウンタビリティ原則を遵守している証拠を監督機関に提供することが求められる限りにおいては、同条に従って文書を保存する必要がある。記録それ自体が個人データを含まない場合は、明らかに GDPR の記録保存の制限の原則[46]は適用されない。

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 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.
これらの詳細に加えて、第 29 条作業部会は、管理者がまた侵害について行った判断の根拠も文書化することを勧告する。とりわけ侵害の通知をしない場合は、その判断を正当化する根拠を文書化するものとする。これは、管理者が、その侵害が個人の権利及び自由へのリスクをもたらす可能性が低いと判断した理由を含む[47]。一方、管理者が、第 34 条(3)のいずれかの条件が満たされたと判断する場合は、条件を満たすという適切な証拠を提出できるようにするものとする。

[44] See Article 5
第 5 条参照
[45] See Article 6 and also Article 9.
第 6 条及び第 9 条も参照。
[46] See Article 5(1)(e).
第 5(1)(e)条参照
[47] See Recital 85
前文第 85 項参照

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.
管理者が監督機関に違反を通知してはいるがその通知が遅れた場合は、管理者はその遅延の理由を提出できなければならない。これについて文書化することは、報告の遅延が正当であって過度の遅延ではないことを証明する手助けとなりうるものである。

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.
管理者が、侵害について、影響を受ける個人に連絡する場合は、その侵害について透明性が必要であり、効果的かつ適時に連絡する必要がある。従って、これらの連絡の証拠を保管することにより、管理者がアカウンタビリティ及びコンプライアンスを証明する一助となる。

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.
第 33 条及び 44 条の遵守の手助けとするため、管理者と処理者の両方が、通知手順を文書化し、侵害が探知された場合に取るべき手続（事故の阻止、制御及び回復、並びにリスク評価及び侵害の通知含む）を定めることが望ましい。この点について、GDPR の遵守を示すためには、従業員がこれらの手順及びメカニズムの存在について知らされたこと、並びに従業員が侵害への対応方法を知っていることを証明することもまた有用である。

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 Article 83.
侵害を適切に文書化するのを怠った場合、違反に対して監督機関が第 58 条に基づくその権能を行使することになり、かつ、又は、第 83 条に従った制裁金を科されることになりうるということに留意を要する。

B. Role of the Data Protection Officer
B. データ保護オフィサーの役割

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.
管理者又は処理者は、第 37 条の要件により、又は望ましい慣行として自発的に、データ保護オフィサー(DPO)を置くことができる [48]。GDPR 第 39 条は、DPO として必須の一連の職務を定めるが、場合に応じて管理者がさらなる職務を担当させることを妨げない。

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.
特に侵害通知に関連して、DPO の必須の職務としては、その他の義務にもまして、まずは管理者若しくは処理者に対するデータ保護の助言及び情報の提供、GDPR 遵守の監視、並びに DPIAs に関する助言の提供である。DPO はまた、監督機関と協力し、監督機関及びデータ主体にとっての連絡窓口として行動しなければならない。また、侵害を監督機関に通知する際には、第 33 条(3)(b)は管理者がその DPO の氏名及び連絡先詳細、又はその他の連絡窓口を提出するよう求めている。

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.
侵害の文書化において、管理者又は処理者は、この文書化の構成、作成及び管理について DPO の意見を聴くことを希望することもありうる。DPO はまた、これらの記録の保管についてもあわせて担当することもありうる。

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

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
DPO についての WP ガイドライン参照。以下: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

これらの要因は、DPO が、助言の提供及びコンプライアンスの監視により、侵害の阻止又は対策策定の支援、並びに侵害の発生中(すなわち監督機関に通知する時)、またその後の監督機関の調査中において、主要な役割を果たすべきものであることを意味する。この観点からして、第 29 条作業部会は DPO が侵害の存在について直ちに通知を受け、侵害の管理及び通知手続の全体にわたって関与することを勧告する。

VI. Notification obligations under other legal instruments
VI. その他の法的文書に基づく通知義務

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:
GDPR に基づく侵害についての通知と連絡に加えて、またそれとは別に、管理者は、自らに適用されうる他の関連する法制に基づく安全上の事故についての通知要件について、及び、この要件が同時に個人データ侵害につき監督機関に通知することも求めるものかについても知っておくことを要する。このような要件は加盟国間で異なりうるが、他の法的文書における通知要件の例と、これらの法的文書と GDPR との相互関係は、以下のものを含む：

・Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].
・域内市場における電子取引のための電子識別及び信頼役務に関する規制（EU）910/2014（eIDAS 規制）[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 規制の第 19 条(2)は、トラストサービスプロバイダーに、トラストサービスプロバイダー又はそこで保管する個人データに重大な影響を有するセキュリティ侵害又は完全性喪失について、監督機関に通知することを求めている。該当する場合はーすなわち、当該の侵害又は喪失が、GDPR に基づく個人データ侵害でもある場合はートラストサービスプロバイダーはまた監督機関に通知することを要する。

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

・Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].
・欧州連合におけるネットワーク及び情報システムの安全性に関する高度で共通の水準を確保するための措置に関する指令(EU)2016/1148（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 指令の第 14 条及び 16 条は、重要サービス運営者及びデジタルサービスプロバイダーに対して、セキュリティインシデントにつきその所轄官庁に通知するよう求めている。NIS の前文第 63 項が認めるように [51]、セキュリティインシデントは、しばしば個人データに対する被害を含みうる。NIS は、所轄官庁及び監督機関に、その文脈において協力し情報交換をするよう求めている一方で、このようなインシデントが GDPR のもとで個人データ侵害であるか個人データ侵害となる場合は、これらの運営者及びプロバイダーは、NIS のインシデント通知要件とは別途、監督機関に通知することを要するであろう。

Example
事例
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.
NIS 指令のもとでの侵害について通知を行うクラウドサービスプロバイダーは、これが個人データ侵害も含む場合には、管理者にも通知することを要する。同様に、eIDAS のもとで通知をするトラストサービスプロバイダーは、侵害が生じた場合には、関連するデータ保護機関にも通知を要する。

[50] See
以下参照
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."*
前文第 63 項:*「多くの場合において、インシデントの結果として個人データが被害を受ける。この文脈においては、所轄官庁及びデータ保護機関は、インシデントから生ずる個人データ侵害に取り組むため、全ての関連事項において、協力し情報交換するものとする。」*

・Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).
・指令 2009/136/EC（市民権指令）及び規制 611/2013（侵害通知規則）

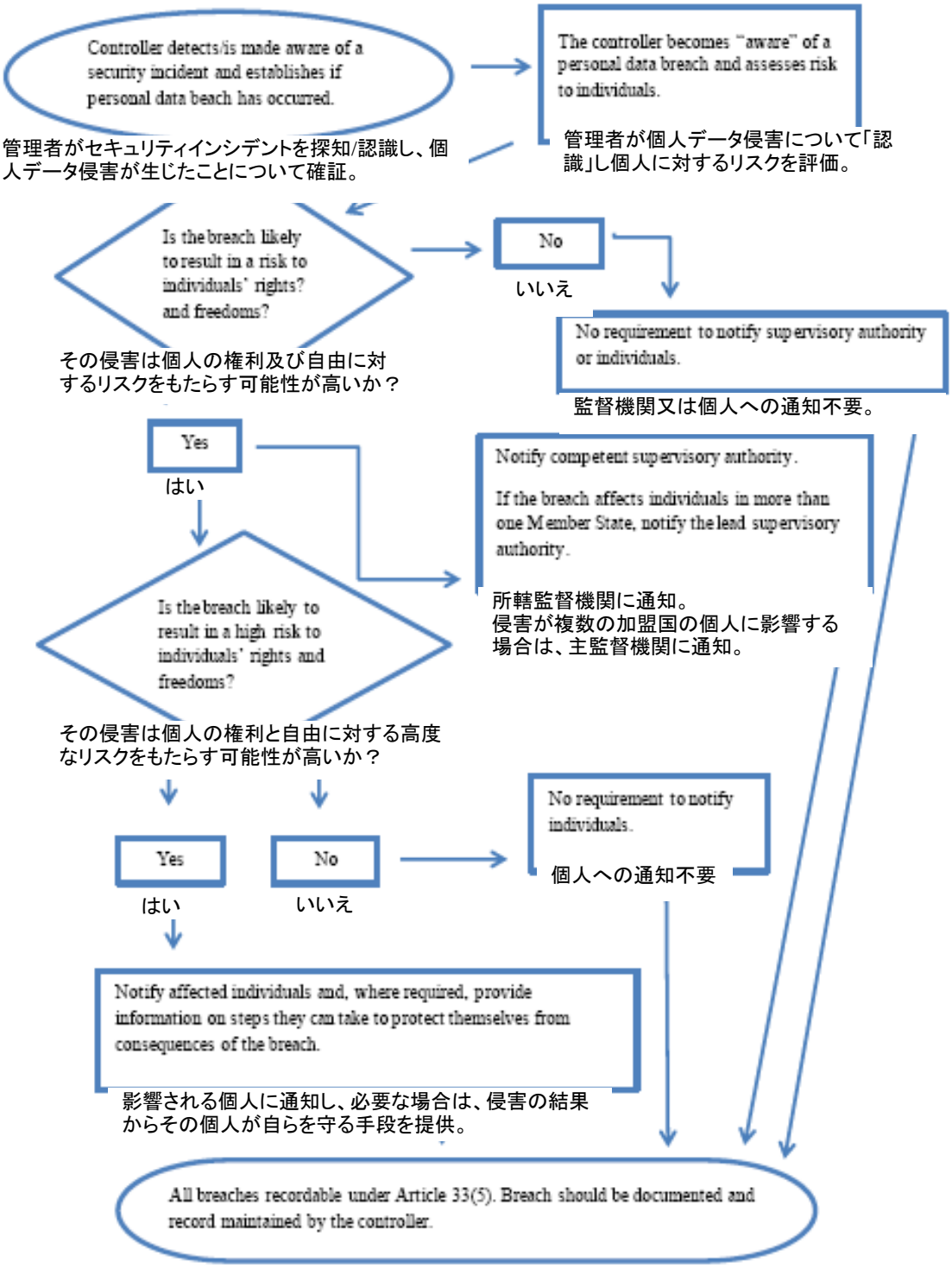
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52] must notify breaches to the competent national authorities.
指令 2002/58/EC[52] の文脈における、公に利用可能な電子通信サービスのプロバイダーは、侵害について所轄の国内官庁に通知しなければならない。

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.
管理者はまた、その他の適用される制度のもとでの、追加的な、法律上、医療上若しくは職業上の通知義務についても認識していることを要する。

VII. Annex
VII. 別紙

A. Flowchart showing notification requirements
A. 通知要件を示すフローチャート

[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, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
2017 年 1 月 10 日、欧州委員会は、指令 2009/136/EC に置き換わり通知要件を取り除く、プライバシー及び電子通信についての規制を提案した。但しこの提案が欧州議会で承認されるまでは、現存の通知要件の効力は継続する。以下参照
https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications



B. Examples of personal data breaches and who to notify

B. 個人データ侵害の例及び通知先

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.
以下の例はすべてを網羅するものではないが、異なる個人データ侵害のシナリオにおいて通知の要否を判断する一助となるものである。これらの例は、また個人の権利及び自由に対するリスクと高度なリスクを区別する手助けともなる。

Example **事例**	**Notify the supervisory authority?** **監督機関に通知するか？**	**Notify the data subject?** **データ主体に通知するか？**	**Notes/recommendations** **注記/勧告**
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. i.ある管理者が、暗号化されたデータのアーカイブのバックアップを USB キーに保管した。休憩中にそのキーが盗まれた。	No. いいえ	No. いいえ	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. データが先端技術のアルゴリズムで暗号化され、データのバックアップが存在し、ユニークキーが害されておらず、データが適時に回復可能である限り、これは報告対象の侵害ではないといいうる。但し後に害された場合は、通知を要する。
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. ii.ある管理者が、オンラインサービスを保持している。そのサービスへのサイバー攻撃の結果として、人の個人データが流	Yes, report to the supervisory authority if there are likely consequences to individuals. はい。個人に影響する可能性が高いならば監督機関に報告すること。	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. はい。影響される個人データの性質に応じて、また個人に対して生じうる結果の重大性が高度ならば、その個人に報告すること。	

出した。 管理者は、単一の加盟国に顧客を有する。			
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. iii.管理者のコールセンターにおける数分間継続する短時間の停電で、顧客が管理者に連絡できず、自らの記録にアクセス不能となっている。	No. いいえ。	No. いいえ。	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller. これは通知対象となる侵害ではないが、第 33 条(5)のもとでの記録対象インシデントではある。 適切な記録を管理者は保管すること。
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. iv.管理者が、全データを暗号化してしまうランサムウェア攻撃を受けている。バックアップは利用できず、データが回復できない。調査したところ、ランサムウェアの唯一の機能は、データの暗号化であり、システムにそれ以外にはマルウェアは現れていないことが判明した。	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability. はい。これは利用可能性の喪失であるため、個人に対する結果が生じる可能性が高い場合は、監督機関に報告すること。	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. はい。影響される個人データの性質、またデータ利用可能性の欠如のおそれ及びその他の生じうる結果に応じて、個人に報告すること。	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. 利用できるバックアップが存在して、適時にデータが回復可能であるならば、利用可能性又は秘密性の恒久的喪失はないから、監督機関に対して、又は個人に対して報告不要。 但し、監督機関がその他の手段により事故を知るに至った場合は、第 32 条のより広範なセキュリティ要件の遵守状況を評

			価するための調査を考慮することがありうる。
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. v.ある個人がデータ侵害を報告するため銀行のコールセンターに電話した。その個人は誰か別人の月次明細書を受領していた。 管理者は、短期的調査(すなわち 24 時間以内に完了)を行い、個人データ侵害が生じたこと、またその他の個人が影響されたかされうるシステム上の欠陥が存在したか否かについて合理的な確信をもってはっきりさせる。	Yes. はい。	Only the individuals affected are notified if there is high risk and it is clear that others were not affected. 高度なリスクがあり、また他の者が影響されないことが明らかな場合、影響を受ける個人のみに通知する。	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. さらなる調査の後に、より多くの人が影響されていることが判明した場合は、監督機関への報告をアップデートしなければならず、他の個人に高度なリスクがあれば、管理者は、他の個人にも通知する追加措置を取る。
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. vi.管理者がオンラインマーケットプレイスを運営し、複数の加盟国に顧客を有し	Yes, report to lead supervisory authority if involves cross-border processing. はい。越境取扱いが関わる場合は、主監督機関に報告すること。	Yes, as could lead to high risk. はい。高度なリスクに至る場合において。	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. 管理者は、措置を取

ている。そのマーケットプレイスがサイバー攻撃を受けて、ユーザー名、パスワード及び購入履歴が攻撃者によりオンラインで公表された。			ることを要する。例えば、影響を受けたアカウントのパスワードのリセットの強制、及びその他のリスクを抑制する手段による。 管理者はまた、その他の通知義務も考慮することを要する。例えば、デジタルサービスプロバイダーとしての、NIS 指令に基づく義務
vii. A website hosting company acting as a 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. vii.データ処理者として活動するウェブサイトホスティング会社が、ユーザー承認を制御するコードにエラーを発見した。この欠陥の影響は、いずれのユーザーも、任意の他のユーザーのアカウントの詳細にアクセスできるということである。	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 investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore 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. 処理者として、ウェブサイトホスティング会社は、不当に遅延することなく、その影響された顧客(管理者)に通知しなければならない。 ウェブサイトホスティング会社が自らの調査を遂行したということを前提とすれば、影響された管理者は、各人が侵害を受けたかどうかについて確信を得たはずであり、よってホスティング会社(処理	If there is likely no high risk to the individuals they do not need to be notified. 個人に対する高度のリスクのおそれがない場合、その個人への通知は不要。	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. ウェブサイトホスティング会社(処理者)は、その他一切の通知義務も考慮しなければならない(例：デジタルサービスプロバイダーとしての、NIS 指令に基づく義務)。 この脆弱性がいずれの管理者についても利用された証拠がないのであれば、通知対処の侵害は起こっていないと言いうるが、記録対象となったり、第 32 条に基づく不遵守問題となる可能性はある。

	者)から通知された時に「認識するに至った」とみなされる可能性がある。その場合、管理者は監督機関に通知しなければならない。		
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack. viii.病院の医療記録がサイバー攻撃により30時間利用不能となった。	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur. はい。病院は、患者の福利及びプライバシーに高度なリスクが生じうるとして通知する義務を負う。	Yes, report to the affected individuals. はい。影響された個人に報告すること。	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients. ix. 多数の学生の個人データが誤って1000 人以上の受信者のあるメーリングリストに送信された。	Yes, report to supervisory authority. はい。監督機関に報告のこと。	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences. はい。含まれた個人データの範囲及び種類、並びに想定される結果の重大性に応じて、個人に報告。	
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. x.ダイレクトマーケティングの電子メールが「to:」若しくは「cc:」欄の受信者に送信され、それにより各受信者は他の受信者の電子メールアドレスを見ることができるようになった。	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) or if other factors present high risks (e.g. the mail contains the initial passwords). はい。多数の個人が影響された場合、センシティブデータが明らかになった場合(例えば、サイコセラピストのメーリングリスト)、又はその他の要因が高度なリスクを示す場合(例えば、メールが初期パスワードを含む場合)、監督機関への通知は義務的となりうる。	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences. はい。含まれた個人データの範囲及び種類、並びに想定される結果の重大性に応じて、個人に報告。	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed. センシティブデータが明らかにされず、また僅かな数の電子メールアドレスしか明らかにされていない場合は、通知は不要でありうる。