仮日本語訳

Guidelines 9/2022 on personal data breach notification under GDPR
GDPR に基づく個人データ侵害通知に関する ガイドライン 9/2022

Version 2.0
バージョン 2.0

Adopted 28 March 2023
2023 年 3 月 28 日採択

本書面は、欧州データ保護会議(EDPB)により 2023 年 3 月 28 日に採択された “Guidelines 9/2022 on personal data breach notification under GDPR” 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。

Version history
バージョン履歴

Version 1.0 バージョン 1.0	10 October 2022 2022 年 10 月 10 日	Adoption of the Guidelines (updated version of the previous guidelines WP250 (rev.01) adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation. 対象を絞ったパブリック・コンサルテーションのためのガイドライン（第 29 条作業部会が採択し、2018 年 5 月 25 日に EDPB が承認した従前のガイドライン WP250 (rev.01) の更新版）の採択。
Version 2.0 バージョン 2.0	28 March 2023 2023 年 3 月 28 日	Adoption of the Guidelines following the targeted public consultation on the subject of data breach notification for controllers not established in the EEA. EEA 域内に拠点のない管理者のデータ侵害通知について対象を絞ったパブリック・コンサルテーション後のガイドラインの採択。

TABLE OF CONTENTS
目次

THE EUROPEAN DATA PROTECTION BOARD
欧州データ保護会議は

Having regard to Article 70(1)(e) and (l) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),
個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679(以下「GDPR」という)の第 70 条第 1 項(e)に鑑み、

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],
2018 年 7 月 6 日の EEA 共同委員会の決定 No 154/2018 により改正された EEA 協定 [1]、特にその附属書 XI 及び議定書 37 に鑑み、

Having regard to Article 12 and Article 22 of its Rules of Procedure,
その手続規則の第 12 条及び第 22 条に鑑み、

Having regard to the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01,
第 29 条作業部会の規則 2016/679 に基づく個人データ侵害通知に関するガイドライン、WP 250 rev.01 に鑑み、

HAS ADOPTED THE FOLLOWING GUIDELINES
次のガイドラインを採択する

0 PREFACE
0 序文

1. On 3 October 2017, the Working Party 29 (hereinafter "WP29") adopted its Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01)[2], which were endorsed by the European Data Protection Board (hereinafter "EDPB") at its first Plenary meeting[3]. This document is a slightly updated version of those guidelines. Any reference to the WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) should, from now on, be interpreted as a reference to these EDPB Guidelines 9/2022.
2017 年 10 月 3 日、第 29 条作業部会(以下「WP29」という) は、規則 2016/679 に基づく個人データ侵害通知に関するガイドライン(WP250 rev.01) [2] を採択し、当該ガイドラインは欧州データ保護会議(以下「EDPB」という)により初回の本会議において承認された [3]。今回の文書は、当該ガイドラインに若干の更新を加える

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
当該ガイドライン中の「加盟国」への言及は、「EEA 加盟国」への言及として解釈されたい。

[2] WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) (last revised and updated on 6 February 2018), available at https://ec.europa.eu/newsroom/article29/items/612052.
WP29 の規則 2016/679 に基づく個人データ侵害通知に関するガイドライン(WP250 rev.01)(2018 年 2 月 6 日最終改訂・更新版)は、以下より入手可: https://ec.europa.eu/newsroom/article29/items/612052

[3] See https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en 参照。

ものである。WP29 の規則 2016/679 に基づく個人データ侵害通知に関するガイドライン(WP250 rev.01)への言及は、今後、当該 EDPB ガイドライン 9/2022 への言及として解釈されたい。

2. The EDPB noticed that there was a need to clarify the notification requirements concerning the personal data breaches at non-EU establishments. The paragraph concerning this matter has been revised and updated, while the rest of the document was left unchanged, except for editorial changes. The revision concerns, more specifically, paragraph 73 in Section II.C.2 of this document.
EDPB は、EU 域内に拠点がない場合の個人データ侵害に関する通知要件を明確にする必要性を認識した。この問題に関するパラグラフが改訂及び更新されている一方で、編集上の変更を除いて、今回の文書の残りの部分は元のまま残されている。今回の改訂は、より具体的には、今回の文書の第 II 章第 C 節第 2 項のパラグラフ 73 に関するものである。

INTRODUCTION
はじめに

3. The GDPR introduced the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[4] (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.
GDPR は、個人データ侵害(以下「侵害」とする)を国内の所轄監督機関 [4](越境侵害の場合は、主監督機関)に通知する要件、及び、特定の場合においては、侵害によりその個人データが影響を受けている個人に連絡する要件を導入した。

4. Obligations to notify in cases of breaches existed 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)[5]. There were also some Member States that already had their own national breach notification obligation. This might included 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 might had relevant Codes of Practice (for example, in Ireland[6]). Whilst a number of EU data protection authorities encouraged controllers to report breaches, the Data Protection Directive 95/46/EC[7], which the GDPR replaced, did not contain a specific breach notification obligation and therefore such a requirement was new for many organisations. The GDPR makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[8]. Processors also have

---

4 See Article 4(21)GDPR.
GDPR 第 4 条(21)参照 。

5 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 。

6 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。

7 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。

8 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、以下より入手可: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

an important role to play and they must notify any breach to their controller[9].
公衆に利用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、(指令 2009/136/EC 及び(EU)規則 No. 611/2013 に明示されているとおり)[5] 侵害が生じた場合の通知義務が定められていた。また、既に独自の国内侵害通知義務を定めていた EU 加盟国もあった。これには、公衆に利用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場合の侵害通知義務(例えば、ドイツ及びイタリアの場合)、又は(オランダの場合のように)個人データが関与する全ての侵害を報告する義務も含まれよう。関連する実施規範を定めていた加盟国もあろう(例えば、アイルランドの場合 [6])。複数の EU のデータ保護機関が侵害の報告を管理者に推奨していた一方で、GDPR が取って代わったデータ保護指令 95/46/EC[7] は、特定の侵害通知義務を定めていなかったため、このような通知要件は、多くの組織にとって新たな要件であった。GDPR は、侵害が個人の権利及び自由 [8] に対するリスクを発生させるおそれがない場合を除き、全ての管理者に対し通知を義務としている。処理者もまた重要な役割を担っており、処理者は自身の管理者に対し侵害を通知しなければならない [9]。

5. The EDPB considers that the 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[10]. 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 GDPR a possible sanction is applicable to the controller.
EDPB は、通知要件には多くの利点があると考えている。管理者は、監督機関に通知する場合、影響を受ける個人に知らせ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、侵害について個人に知らせるよう管理者に命令することができる [10]。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について、また個人がその生じうる影響から自身を守るために講ずることのできる手立てについて、情報を提供することが可能になる。侵害対応計画の焦点は、個人及びその個人データの保護に当てられなければならない。その結果、侵害通知は、個人データの保護に関する規則の遵守を強化するための道具とみなされるはずである。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なければならない。

6. 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[11], 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 [11]、その後に所轄監督機関に対する通知の要否、また必要な場合関連する個人に対する侵害の連絡の要否を判断す

---

[9] 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、(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が、個人データの侵害が生じた場合、契約プロバイダーに対し通知する義務がある旨を定める(EU)規則 No 611/2013 の第 5 条の概念に類似している。

[10] See Articles 34(4) and 58(2)(e) GDPR.
GDPR 第 34 条(4)及び第 58 条(2)(e)参照。

[11] 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)[)].
これは、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おそれがある取扱業務に対し求められる、DPIA の実施及び評価の見直しの要件に基づき確保することが可能である(第 35 条(1)及び(11))。

ることを可能にするような工程を事前に計画し、整備しておくことが推奨される。監督機関に対する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。

7. 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 には、どのような場合に通知が要求されるか、また誰に対してか、加えて通知の一環としてどのような情報を提供すべきかについての規定がある。通知が要求される情報は、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、全ての侵害に対し適時に対応しなければならない。

8. In its Opinion 03/2014 on personal data breach notification[12], 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.
個人データ侵害の通知に関する意見 03/2014[12] において、WP29 は管理者に対し、侵害が生じた場合データ主体に対する通知をするか否かの決定の助けとなるようなガイダンスを提供している。当該意見書は、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、当時の GDPR 草案に照らし複数の産業分野における事例を挙げ、全ての管理者について望ましい慣行を提示している。

9. 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 obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.
このガイドラインは、GDPR の義務である侵害の通知及び連絡の要件、並びに当該義務を遵守するために管理者及び処理者が講じうる措置の一部について説明している。また、様々な種類の侵害及び異なる状況下において誰に対し侵害の通知が必要となるかについての事例を提示している。

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. 基本的な安全性の考察

10. 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[13].
GDPRは、適切な技術的及び組織的措置を講ずることにより、無権限又は違法な取扱い、及び、偶発的な喪失、破壊又は損壊に対する保護を含め、個人データの適切な安全性を確保する態様により、個人データを取り扱うことを要件の一つとしている[13]。

11. 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,

[12] See WP29 Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
WP29 の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/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[13] See Articles 5(1)(f) and 32 GDPR.
GDPR 第 5 条(1)(f)及び第 32 条参照。

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[14]. Also, the GDPR requires all appropriate technological protection an[d] organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[15].
したがって、GDPR は、取り扱われる個人データがさらされるリスクに適切に対応する、一定レベルの安全性を確保するための適切な技術的及び組織的な措置を整備しておくよう、管理者及び処理者の両者に要求している。管理者及び処理者は、最新技術、実装費用、取扱いの性質、範囲、過程及び目的並びに自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮しなければならない [14]。また、GDPR は、侵害が生じたか否かを速やかに確証し、その後通知義務が関与するか否かを判断するための、あらゆる適切な技術的保護及び組織的措置を設けておくよう要求している [15]。

12. Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.
結果的に、全てのデータセキュリティ方針の主要な要素は、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、適時に対応することができることである。

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

1. Definition
1. 定義

13. 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「個人データ侵害」を次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」*

14. 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）」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）」については、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されるであろう。最後に、無権限又は違法な取扱いには、

[14] Article 32; see also Recital 83 GDPR.
GDPR 第 32 条、前文第 83 項も参照。
[15] See Rectical 87 GDPR.
GDPR 前文第 87 項参照。

データを受取る権限を持たない取得者に対する個人データの開示（若しくはデータにアクセスする権限を持たない取得者による個人データへのアクセス）、又は GDPR に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、管理者の顧客のデータベースのコピーが入っているデバイスの紛失又は盗難の場合が含まれうる。また、個人データ一式の唯一のコピーが、ランサムウェアにより暗号化される場合、又は管理者により暗号化されたものの、暗号化に用いた鍵を管理者が所有しなくなる場合も喪失の事例となりうる。

15. 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 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[16].
侵害は、セキュリティインシデントの一種であることを明らかにしておかなければならない。GDPR 第 4 条(12)が示すように、GDPR は、個人データの侵害が存在する場合にのみ適用される。そのような侵害の結果、管理者が GDPR 第 5 条に概説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することができなくなるということである。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強調するものである。つまり、個人データ侵害は全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、必ずしも全て個人データ侵害であるとは限らないということである [16]。

16. The potential adverse effects of a breach on individuals are considered below.
侵害により生じうる個人に対する悪影響について、以下で考察する。

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

17. 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[17]:
WP29 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次の三つの情報セキュリティ原則に基づき分類可能であると説明している [17]。

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- 「機密性の侵害」—個人データに対する無権限の又は偶発的な開示又はアクセスがある場合。

- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- 「完全性の侵害」—個人データに対する無権限の又は偶発的な改変がある場合。

[16] 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、セキュリティ原則に違反する内部取扱いに起因するインシデントを含むことに留意しなければならない。

[17] See WP29 Opinion 03/2014.
WP29 の意見 03/2014 参照。

- “Availability breach” - where there is an accidental or unauthorised loss of access[18] to, or destruction of, personal data.
- 「可用性の侵害」—個人データに対する偶発的又は無権限のアクセス[18]の喪失又は破壊がある場合。

18. 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、侵害が個人データの機密性、完全性及び可用性の全てに関与する場合、及びこれらのいずれかの組合わせにより関与する場合があり得ることについても留意しなければならない。

19. 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生じたか否かの判断は比較的明らかであるが、可用性の侵害が生じたか否かの判断はそれほど明白ではないかもしれない。個人データの恒久的な喪失又は破壊が生じる場合、侵害は常に可用性の侵害とみなされる。

> 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.
> 可用性の喪失の例には、データが偶発的に若しくは権限を持たない者により消去された場合、又は安全に暗号化されたデータの例では、復号鍵を喪失した場合が含まれる。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、これは恒久的な可用性の喪失とみなされる。
>
> 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、例えば停電又はサービス拒否攻撃が発生し、個人データが利用できなくなるといった、組織の通常サービスに対する重大な支障が発生する場合にも起こりうる。

20. 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 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*

[18] It is well established that “access” is fundamentally part of “availability”. See, for example, NIST SP80053rev4, which defines “availability” as: "Ensuring timely and reliable access to and use of information," available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: “Timely, reliable access to data and information services for authorized users”. See https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines “availability” as “Property of being accessible and usable upon demand by an authorized entity”: https://www.iso.org/obp/ui/#iso:std:isoiec: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。例えば、NIST SP800-53rev4 は、「可用性」を「適時に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。以下より入手可：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. また、CNSSI-4009 は、「権限を有する者によるデータ及び情報サービスへの適時かつ確実なアクセス」と言及している。https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf.参照。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 参照。

restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".
個人データの一時的な可用性の喪失は侵害とみなされるか否か、また侵害とみなされる場合、通知が必要となる侵害とみなされるか否かという疑問が生じうる。GDPR 第 32 条の「取扱いの安全性」は、リスクに適切に対応する一定のレベルの安全性を確保するための適切な技術上及び組織上の措置を実装する際、特に、*「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」*を考慮しなければならない旨、説明している。

21. 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) GDPR.
したがって、一定時間個人データの使用が不可能となるセキュリティインシデントもまた、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、侵害の一種である。明らかなことであるが、計画的なシステムメンテナンスの実行により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『安全性に対する侵害』ではない。

22. 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) GDPR. This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[19]. 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 GDPR, 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）の場合と同様に、第 33 条(5)に従い一時的な可用性の喪失が関与する侵害を文書化しておかなければならない。このことは、管理者が、当該記録の閲覧を求める可能性のある監督機関[19]に対し、アカウンタビリティを証明する際に役立つ。一方、侵害の状況により、監督機関への通知及び影響を受ける個人への連絡が要求される場合とそうでない場合がある。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蓋然性と深刻度を評価する必要がある。GDPR 第 33 条に従い、侵害が個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、管理者は通知する必要がある。当然ながら、これはケースごとに評価する必要がある。

Example 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.
病院の関係では、患者に関する重要な医療データが、一時的にでも、使用できない場合、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。例えば、手術が中止となり、生命が危険にさらされうる場合。

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.
逆に、メディア企業のシステムが数時間利用不能になり（例えば、停電による利用不能）、当該企業が購読者へのニュースレターの送信を妨げられる場合、このことにより個人の権利及び自由に対するリスクが生じ

[19] See Article 33(5) GDPR.
GDPR 第 33 条(5)参照。

るおそれはない。

23. 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が一時的なものに留まるかもしれず、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要求される場合もあるため、侵害により生じう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しなければならない。

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のあるソフトウェア）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、一時的な可用性の喪失に帰結する可能性がある。一方、さらにネットワークへの侵入が生じており、当該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ること）となり、このことにより個人の権利及び自由に対するリスクが生じる場合、通知が要求される可能性がある。

3. The possible consequences of a personal data breach
3. 個人データ侵害により生じうる結果

24. 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[20].
侵害は、個人に対し様々な種類の重大な悪影響を及ぼす可能性がある。このような悪影響は、物的な損失、財産的な損失若しくは非財産的な損失をもたらしうる。GDPR は、これには自身の個人データに対する管理の喪失、個人の権利の制限、差別、ID 盗取又は ID 詐欺、金銭上の損失、無権限による仮名の復元、信用の毀損、職務上の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うると説明している。これにはまた関係す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うる [20]。

25. 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[21].
よって、GDPR は、そのような悪影響が起きるリスクのおそれがない場合を除き、所轄監督機関に対する侵害の通知を管理者に要求している。このような悪影響が起きる高いリスクのおそれがある場合、GDPR は、影響を受ける個人に対する合理的に可能な限り速やかな侵害の連絡を管理者に要求している [21]。

26. 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:

[20] See also Recitals 85 and 75 GDPR.
GDPR 前文第 85 項及び第 75 項も参照。
[21] See also Recital 86 GDPR.
GDPR 前文第 86 項も参照。

侵害を特定し、個人に対するリスクを評価したうえで、必要に応じ通知を実施することを可能にしておく重要性については、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。」*

27. Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.
個人に対する悪影響のリスク評価に関する更なる指針については、第 IV 章で考察する。

28. 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 GDPR 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[22], either accompanying a corrective measure under Article 58(2) GDPR 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 GDPR) on the one hand, and absence of (adequate) security measures (Article 32 GDPR) on the other hand, as they are two separate infringements.
GDPR 第 33 条及び／又は第 34 条の要件が満たされているにもかかわらず、管理者がデータ侵害について、監督機関若しく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、監督機関には、その裁量によりあらゆる是正措置の検討を含めるべく選択肢がある。これには、第 58 条(2)に基づく是正措置を伴うか又は単独での、適切な制裁金 [22] を科すことの検討が含まれる。制裁金を科すことを選択する場合、その金額は GDPR 第 83 条(4)(a)に基づき、1,000 万ユーロ以下又は世界全体における年間売上総額の 2%以下の金額とすることができる。また場合によっては、侵害の通知の懈怠が、既存の安全管理措置の欠如又は不足を露呈している可能性があることに留意しておくことも重要である。WP29 の制裁金に関するガイドラインは、*「単一の事案におい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」*と定めている。この場合、監督機関は、侵害の通知又は連絡（第 33 条及び 34 条）の懈怠に対し制裁を科す一方で、（十分な）安全管理措置（第 32 条）の欠如に対し制裁を科す可能性もある。なぜなら、これらは2つの

[22] 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、WP29 の制裁金の適用及び設定に関するガイドラインを参照のこと。以下より入手可：http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

別個の違反行為だからである。

II. ARTICLE 33 - NOTIFICATION TO THE SUPERVISORY AUTHORITY
II. 第 33 条 – 監督機関に対する通知

A. When to notify
A. 通知する場合

1. Article 33 requirements
1. 第 33 条の要件

29. Article 33(1) GDPR provides that:
GDPR 第 33 条(1)は、次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。」*

30. Recital 87 GDPR states[23]:
GDPR 前文第 87 項は、次のように定めている[23]。

> *"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。」*

2. When does a controller become "aware"?
2. 管理者が「認識」した時点とは？

31. As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach

[23] Recital 85 GDPR is also important here.
ここでは GDPR 前文第 85 項も重要である。

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. The EDPB 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.
先に詳述したように、GDPR は、個人データ侵害が発生した場合、管理者は、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、その侵害を通知するよう、要求している。このことは、いつ管理者が侵害を「認識」したとみなされうるかという疑問を提示しうる。EDPB は、管理者が、個人データの侵害につながるセキュリティ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で「認識」したとみなされるであろうと考えている。

32. 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[24]. 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、先に示したように、GDPR は、侵害が発生したかどうかを迅速に確証するために、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に、全ての適切な技術的な保護及び組織上の措置を実装するよう管理者に要求している。また、その侵害の性質及び重大性、並びに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、不当に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とも定めている [24]。これは、管理者が適切な措置を講ずることができるよう、あらゆる侵害を適時に「認識」することを確保しておく義務を管理者に課すものである。

33. When, exactly, a controller can be considered to be “aware” of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.
どの時点で、正確に、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。侵害が生じたということが初めから比較的明らかである場合もあろうが、一方で、個人データが侵害されたかについて確証するのに時間がかかる場合もある。しかし、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、必要に応じて通知するといった対応を迅速に行うことである。

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が入っている USB キーを紛失した場合、権限を持たない者が当該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。一方、管理者が機密性の侵害が生じたか否かについては確証できない場合でも、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ようなケースは、通知しなければならない。このとき管理者は、USB キーの紛失に気付いた時点で侵害を「認識」したことになるであろう。

[24] See Recital 87 GDPR.
GDPR 前文第 87 項参照。

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. ある第三者が管理者に対し、当該管理者の顧客の一人の個人データを偶発的に受領したことを通知し、かつ無権限の開示の証拠を提供する。管理者はこのとき、機密性の侵害の明らかな証拠を提示されているため、侵害を「認識」したことに疑いの余地はない。

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. ある管理者が自身のネットワークへの侵入の可能性を検知する。管理者はシステムに保存されている個人データが侵害されているか否かを確証するために当該システムを調査し、侵害されていることを確認する。ここでも、管理者はこの時点で侵害の明らかな証拠を得ているため、侵害を「認識」したことに疑いの余地はない。

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. あるサイバー犯罪者が、管理者のシステムをハッキングした後、当該管理者に身代金を要求するために連絡する。このケースでは、管理者が自身のシステムを調査し、システムが攻撃されたことを確認した後、管理者は侵害が生じた明らかな証拠を得ており、侵害を「認識」したことに疑いはない。

34. 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、メディア組織若しく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、又はセキュリティインシデントを独自に検知したとき、侵害が実際に生じているか否かを確証するために、短期間の調査を実施しうる。当該調査期間中、管理者は、侵害を「認識」しているとみなされないかもしれない。一方、初期調査は、可及的速やかに開始し、侵害が生じているか否かについて合理的な程度の確信をもって確証するよう期待される。より詳細な調査は、その後引き続き実施できる。

35. 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)[25] 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.
管理者が侵害を認識したとき、通知が要件となる侵害については、不当に遅滞することなく、かつ、それが実施可能なときは、72 時間以内に通知しなければならない。この期間中、管理者は、通知要件が発生しているか否かを確証し、また侵害への対応に必要な（複数の）措置を判断するために、個人に対して生じ得

[25] See WP29 Guidelines WP248 on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
WP29 の DPIA に関するガイドライン WP248、以下を参照：
http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

るリスクを評価しなければならない。一方、管理者は、該当の取扱い活動を開始する前に行うデータ保護影響評価（DPIA）[25] の一環として、侵害の結果生じる可能性のあ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時の特定の状況下での評価に比べ、より一般的な評価となるかもしれない。よって、いかなる場合においても、特定の状況を考慮した追加的な評価を実施することが必要となる。リスク評価に関する詳細については、第 IV 章を参照のこと。

36. 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.
多くの場合、このような初期段階の対応は、最初の警告（つまり、管理者又は処理者が、個人データが関与しうるセキュリティインシデントが生じたことを疑う時点）後、速やかに完了しなければならない。例外的な場合のみ、より長い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.
ある個人がその管理者に対し、当該管理者になりすました電子メールを受け取った旨、報告する。当該電子メールには、顧客自身が（実際に）使用した、当該管理者が提供するサービスに関する個人データが含まれていた。これは当該管理者のセキュリティが侵害されていることを示唆している。当該管理者は短期間の調査を行い、自身のネットワークへの侵入及び個人データへの無権限のアクセスの証拠を特定する。管理者は、この時点で侵害を「認識」したとみなされ、このことが個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、監督機関に対する通知が要求される。管理者は、侵害に対応するための適切な救済措置を講ずる必要がある。

37. 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[26]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.
したがって管理者は、侵害を検知し対応することができるよう、組織内でのプロセスを整備しておかなければならない。例えば、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措置を使用しうる。様々なログデータ [26] を相関させることで、これらから事象及び警告を明確化することが可能になる。侵害が検知された際、当該侵害に対応できるように適切なレベルの管理職員に上申すること、また、要すれば、第 33 条に従った通知、かつ必要な場合、第 34 条に従った連絡をすることが重要である。このような措置及び報告メカニズムは、管理者のインシデント対応計画及び／又はガバナンスの取決め書に詳細に定めておくことが可能であろう。これらは、管理者が、組織内における侵害対応の業務上の責任者について、また適切なインシデントの上申方法又は

[26] 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.
監査能力を向上する、データの保管、変更又は消去等のログデータも、各々の取扱業務を開始した者に関する個人データとみなされうることに留意しなければならない。

上申の要否について、効果的に計画し、決定するのに役立つ。

38. 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).
管理者はまた、管理者が使用する全ての処理者と、侵害が発生した場合、処理者自身が管理者に通知する義務を負うという合意を取り交わしておかなければならない（以下参照）。

39. 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.
侵害を防止し、検知し、また対応ができるよう適切な措置を整備しておくことは、管理者及び処理者の責任であるが、どのような場合においても講ずべき実用的な手順が存在する。

- 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.
- 全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職務とする責任者又は担当者に報告する。

- 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.
- その後、報告を受けた組織の関連部署とともに、侵害の結果生じる個人に対するリスクを評価する（リスクが生じ無い、リスクが生じる、又は高いリスクが生じる蓋然性）。

- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- 要求される場合、監督機関に対する通知、及び可能性としては影響を受ける個人に対する侵害の連絡。

- At the same time, the controller should act to contain and recover the breach.
- 同時に、管理者は、侵害を阻止し及び復旧するための措置を講ずる。

- Documentation of the breach should take place as it develops.
- 侵害の進展に応じて当該侵害を文書化する。

40. 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) GDPR have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[27]. 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 GDPR.
したがって、最初の警告で対応し、侵害が実際に生じたか否かを確証するのは管理者側の義務であるということは明らかである。この短期間である程度の調査が可能になり、管理者は、証拠及びその他の関連の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もって、侵害が生じたと確証した後、第 33 条(1)に規定する条件が満たされる場合、管理者は、不当な遅滞なく、かつ、それが実施可能なときは、72 時間以内に [27] 監督機関に対し、通知しなければならない。管理者が適時に対応せず、侵害が実際に生じていたことが明白になった場合、このことは GDPR 第 33 条に基づく通知の懈怠とみなさ

[27] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN
期間、期日及び時間制限に適用されるルールを定める規則 No. 1182/71 参照。以下より入手可：http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

れる可能性がある。

41. Article 32 GDPR 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.
GDPR 第 32 条は、管理者及び処理者が、個人データに対する一定のレベルの安全性を確保するために、適切な技術上及び組織上の措置を整備しておかなければならないことを明白にしている。つまり、適時に侵害を検知し、対処し、また報告することを可能にしておくことは、当該措置の必須の要素とみなされるはずである。

3. Joint controllers
3. 共同管理者

42. Article 26 GDPR concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[28]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34 GDPR. The EDPB 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.
GDPR 第 26 条は共同管理者に関するものであり、共同管理者は、GDPR を遵守するため、管理者それぞれの責任について定めておくよう明示している[28]。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。EDPB は、共同管理者間の契約上の合意の中に、いずれの管理者が 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かを定める条項を含めておくよう勧告する。

4. Processor obligations
4. 処理者の義務

43. 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) GDPR 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".
管理者が個人データの保護に対する全体的な責任を保持するが、処理者には、管理者がその義務を遵守できるよう果たすべき重要な役割があり、これには侵害の通知が含まれる。実際、GDPR 第 28 条(3)は、処理者による取扱いは、契約又はその他の法律行為によって規律されると定めている。第 28 条(3)(f)は、当該契約又はその他の法律行為は、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」よう定めるものとする旨、明示している。

44. Article 33(2) GDPR 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

[28] See also Recital 79 GDPR.
GDPR 前文第 79 項も参照。

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.
GDPR 第 33 条(2)は、処理者が管理者により使用されており、かつ、処理者が管理者の代わりに取り扱っている個人データに対する侵害を認識した場合、処理者は、「不当な遅滞なく」管理者に通知しなければならないことを明らかにしている。処理者は、侵害を管理者に通知する前に、まず侵害により生じるリスクの蓋然性を評価する必要がないことに留意しておかなければならない。侵害を認識したとき、このような評価を実施しなければならないのは管理者である。処理者に要されるのは、侵害が生じたか否かを確証し、管理者に通知することだけである。管理者は、自身の目的を達成するために処理者を利用する。したがって、原則、管理者は、処理者が管理者に対し侵害を報告した時点で、侵害を「認識」したものとみなされるはずである。処理者に課される管理者への通知義務により、管理者は、侵害に対応し、第 33 条(1)に従い監督機関に対し、また第 34 条(1)に従い影響を受ける個人に対し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。処理者は該当事案に関係する全ての関連事実を認識できる立場にない場合もあるため、管理者もまた侵害を調査することを望むかもしれない。例えば、処理者が破壊又は紛失した個人データのコピー又はバックアップを管理者が保持している場合。このことは管理者が通知する必要があるか否かについて影響を与えうる。

45. 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, the EDPB 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、処理者は「不当な遅滞なく」通知しなければならないということ以外、処理者が管理者に対し警告しなければならない期限について、明示的に定めていない。よって、EDPB は、処理者は管理者に対し侵害について速やかに通知するよう、追加的情報はより詳細が明らかになる時点で段階的に提供するよう勧告する。このことは、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。

46. 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、GDPR のその他の条項に加えて、第 33 条(2)に明示されている要件を満たす方法を定めておくのがよいであろう。これには、72 時間以内に監督機関に報告するという管理者の義務を助けるような、処理者による早期の通知の要件が含まれうる。

47. 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.
処理者が複数の管理者にサービスを提供しており、全ての管理者が同一のインシデントにより影響を受ける場合、処理者は、それぞれの管理者に対しインシデントの詳細を報告しなければならない。

48. 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 GDPR. However, it is important to note that the legal responsibility to notify remains with the controller.
管理者が処理者に対し適切な権限を与えており、かつ、このことが管理者と処理者間の契約上の合意の一部を成す場合、処理者は管理者の代わりに通知を行うことが可能となる。このような通知は、GDPR 第 33

条及び 34 条に従い行われなければならない。ただし、通知を行う法的責任は管理者が負うということに留意しておくことが重要である。

B. Providing information to the supervisory authority
B. 監督機関に対する情報の提供

1. Information to be provided
1. 提供する情報

49. When a controller notifies a breach to the supervisory authority, Article 33(3) GDPR states that, at the minimum, it should:
管理者が監督機関に対し侵害を通知する場合、GDPR 第 33 条(3)は、最低限、管理者は次の事項を通知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;*
> *「(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) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
> *(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) describe the likely consequences of the personal data breach;*
> *(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) 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."*
> *(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。」*

50. The GDPR does not define categories of data subjects or personal data records. However, the EDPB 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、データ主体の類型又は個人データ記録の種類について定義していない。しかし、EDPB は、データ主体の類型について、その個人データが侵害により影響を受ける様々な類型の個人を指すよう提言する。使用される表現により、これには、とりわけ、子どものほか脆弱性のあるもの、障害のある人々、被雇用者、又は顧客が含まれる場合がある。同様に、個人データ記録の種類について、健康に関するデータ、教育に関する記録、公的介護情報、財務情報、銀行口座番号、パスポート番号等、管理者が取り扱いうる様々な種類の記録を指す場合がある。

51. Recital 85 GDPR 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.
GDPR 前文第 85 項は、通知の目的の一つは、個人に対する損害を抑えることであることを明らかにしている。よって、データ主体の類型又は個人データの種類が、侵害の結果として発生する特定の損害のリスクを示唆する場合（例えば、ID 盗取、ID 詐欺、金銭上の損失、職務上の守秘義務に対する脅威）、通知において、当該類型を示すことが重要である。このように、このことは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要件に関連している。

52. 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（例えば、影響を受けるデータ主体の正確な数）が入手できない場合、このことが適時の侵害の通知の障壁となってはならない。GDPR は、影響を受ける個人の数及び関係する個人データ記録の数について、概算とすることを許可している。正確な数値を提供することよりも、侵害による悪影響に対処することに焦点を当てるべきである。

53. 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.
したがって、侵害が生じたことが明らかになったが、その侵害の範囲がまだ定かではない場合、段階的通知（以下参照）が、通知義務を満たすためには安全な方策である。

54. Article 33(3) GDPR 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.
GDPR 第 33 条(3)は、管理者は通知とともに「少なくとも」この情報を提供するものと定めているため、管理者は、必要な場合、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。異なる侵害の種類（機密性、完全性又は可用性）により、それぞれのケースの状況を完全に説明するために追加的な情報の提供が要求されるかもしれない。

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.
侵害の根本的要因が処理者である場合、特に、これ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記録に影響するインシデントにつながる場合、監督機関への通知の一環として、管理者は、当該処理者の名称を通知することが有益である場合がある。

55. 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、追加的な詳細情報を要求しうる。

2. Notification in phases
2. 段階的通知

56. 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) GDPR therefore states:
侵害の性質により、インシデントに関連する全ての事実をはっきりさせるために、管理者による追加的な調査が必要となる場合がある。よって、第 33 条(4)は、次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、その状況に応じて提供できる。」

57. 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) GDPR. The EDPB 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.
このことは、GDPR は、管理者が侵害を認識したときから 72 時間以内に侵害に関する全ての必要な情報を取得できるわけではないことを認識していることを意味する。こういった初期の段階では、インシデントの完全かつ包括的な詳細情報を必ずしも入手できるとは限らないからである。故に、GDPR は段階的通知を許容している。これは、ある種類のサイバーセキュリティインシデント等、より複雑な侵害の場合に当てはまる可能性がある。例えば、侵害の性質及び侵害された個人データの範囲を完全に確証するために詳細なフォレンジック調査が必要となる場合である。この結果、多くの場合、管理者は後の時点で追加情報を用いて更なる調査及びフォローアップを行う必要がある。これは、GDPR 第 33 条(1)に従い、管理者がその遅滞の理由を提示することを条件に許容される。EDPB は、管理者が監督機関に最初に通知する際に、要件である全ての情報をまだ入手しきれておらず、詳細情報を後に提供する予定であるかどうかについても監督機関に通知するよう勧告する。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しなければならない。このことは、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的な関連情報を認識した場合、管理者が他の時期に追加的な情報を提供することを妨げるものではない。

58. 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.
通知要件の焦点は、管理者が、侵害に迅速に対応し、侵害を阻止し、可能な場合には侵害された個人データを復旧すること、また、監督機関に対し関連する助言を求めることを奨励することにある。最初の 72 時間以内の監督機関への通知により、管理者は、個人に通知するか否かの決定が正しいかを確認することが可能となる。

59. 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[29] 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

[29] See Article 9 GDPR.
GDPR 第 9 条参照。

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.
一方、監督機関への通知の目的は、単に影響を受ける個人に通知するか否かについてのガイダンスを得ることではない。侵害の性質及びリスクの深刻度により、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である場合もある。例えば、ID 盗取の喫緊の脅威が存在する場合、又は特別な種類の個人データ[29]がオンラインで開示される場合、管理者は、侵害を阻止し、当該侵害を関係する個人に連絡すべく、不当に遅滞なく対応しなければならない（第 III 章参照）。例外的状況においては、監督機関に通知する前に、これが行われる場合がある。より一般的に言えば、監督機関への通知は、データ主体への侵害の連絡が要求される場合に連絡をしないことを正当化するものではないということである。

60. 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、最初の通知を行った後、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追加的な調査により明らかになる場合、監督機関に対し情報を更新することが可能であることも明らかであろう。この情報は監督機関に既に提供されている情報に追加され、当該インシデントはそれに応じて侵害に至らなかったものとして記録される可能性がある。最終的に侵害に至らなかったインシデントを報告する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、数名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、侵害を検知してから 72 時間以内に監督機関に通知する。その後、当該 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判明し、発見される。管理者は、監督機関に対し情報を更新し、先の通知が修正されるよう要求する。

61. 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.
通知を段階的に行うやり方は、指令 2002/58/EC、規則 611/2013 及びその他の自己申告型インシデント報告の既存の義務に基づき、既に適用されていることに留意しておくべきであろう。

3. Delayed notifications
3. 通知の遅滞

62. Article 33(1) GDPR 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、監督機関に対する通知が 72 時間以内に行われない場合、その通知には、その遅滞の理由を付すことを明らかにしている。これは、段階的通知の概念に加えて、管理者が常にそのような時間内に侵害を通知できるわけではないこと、また通知の遅滞が許容される場合があることを認識しているものである。

63. 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.
このような事態は、例えば、短期間に複数の同様の機密性の侵害が管理者に生じ、同一の方法で多数のデータ主体に影響を与える場合に発生する可能性がある。管理者は、侵害を認識する可能性があり、調査を開始する一方で、通知を行う前の段階で、異なる原因の同様の追加的な侵害を検知する場合がある。状況により、管理者は侵害の範囲を確証するのに時間がかかる場合があり、各侵害を個別に通知する代わりに、原因が異なり得るが複数の非常に類似した侵害を代表して一つの意味のある通知に整理する。こうすることで、管理者が最初に当該侵害を認識してから 72 時間以上を要し、監督機関に対する通知が遅滞することにつながる可能性がある。

64. 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、個々の侵害が報告を要されるインシデントである。一方、過剰な負担を避けるため、管理者は、複数の侵害が比較的短期間に発生した、同一の方法での同一の種類の個人データの侵害に関するものであることを条件に、関係する全ての侵害を代表して一つの「まとまった」通知を提出することができうる。異なる方法で侵害された、異なる種類の個人データに関する一連の侵害が生じる場合、通知は通常の方法で進めなければならず、第 33 条に従い侵害ごとに報告しなければならない。

65. 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 はある程度の通知の遅滞を許容しているが、常に許容されるものとみなされるものではない。72 時間以内に複数の同様の侵害を報告する場合にも、まとまった通知が可能であ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 域内に拠点がない場合の侵害

1. Cross-border breaches
1. 越境侵害

66. Where there is cross-border processing[30] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) GDPR 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[31]. Article 55(1) GDPR says that:
個人データの越境取扱い[30]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しうる。GDPR 第 33 条(1)は、侵害が発生した場合、管理者は、GDPR の第 55 条[31]に従って所轄監督機関に

[30] See Article 4(23) GDPR.
GDPR 第 4 条(23)参照。
[31] See also Recital 122 GDPR.
GDPR 前文第 122 項も参照。

対し通知しなければならない旨を明らかにしている。第 55 条(1)は次のように定めている。

> *"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。」*

67. However, Article 56(1) GDPR states:
但し、GDPR 第 56 条(1)は次のように定めている。

> *"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."*
> *「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。」*

68. Furthermore, Article 56(6) GDPR states:
さらに、GDPR 第 56 条(6)は次のように定めている。

> *"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。」*

69. 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[32]. 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[33]. 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、侵害が越境取扱いの過程で生じ、かつ通知が要求される場合はいつでも、管理者は主監督機関 [32] に通知する必要があるということを意味する。したがって、侵害対応計画の策定の際、管理者は、どの監督機関が自らが通知しなければならない主監督機関なのかについて評価しなければならない[33]。これにより管理者は、侵害に迅速に対応し、第 33 条に関する義務を果たすことが可能となる。越境取扱いを伴

[32] 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
WP29 の管理者又は処理者の主監督機関の特定についてのガイドライン参照。以下より入手可: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] A list of contact details for all European national data protection authorities can be found at: https://edpb.europa.eu/about-edpb/about-edpb/members_en
欧州諸国データ保護機関全般の連絡先リストは、以下を参照: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

う侵害が生じた場合、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所在する場所、又は実際に侵害が起きている場所とは限らないということを明らかにしておかなければならない。主監督機関に通知する際、管理者は、適切な場合には、該当の侵害が他の加盟国に所在する拠点を含んでいるか、またどの加盟国のデータ主体が当該侵害による影響を受けるおそれがあるかについて明示しなければならない。管理者が主監督機関を特定することに関し疑問がある場合は、最低限、その侵害が生じている現地の監督機関に通知しなければならない。

2. Breaches at non-EU establishments
2. EU 域内に拠点がない場合の侵害

70. Article 3 GDPR 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) GDPR states[34]:
GDPR 第 3 条は、GDPR の地理的適用範囲に関するものであり、EU 域内に拠点の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を含んでいる。特に、GDPR 第 3 条(2)は次のように定めている[34]。

> *"This Regulation applies to the processing of personal data of data subjects who are in the Union by 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。」*

71. Article 3(3) GDPR is also relevant and states[35]:
GDPR 第 3 条(3)も関連条文であり、次のように定めている[35]。

> *"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。」*

72. Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) GDPR and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34 GDPR. Article 27 GDPR requires a controller (and a processor) to designate a representative in the EU where Article 3(2) GDPR applies.
したがって、EU 域内に拠点のない管理者が GDPR 第 3 条(2)又は第 3 条(3)の対象であり、侵害を経験する場合、当該管理者は依然 GDPR 第 33 条及び 34 条に基づく通知義務に拘束されることになる。GDPR 第 27 条は、GDPR 第 3 条(2)が適用される場合、管理者（及び処理者）は、EU 域内における代理人を指定するよう要求している。

---

[34] See also Recitals 23 and 24 GDPR.
GDPR 前文第 23 項及び第 24 項も参照。
[35] See also Recital 25 GDPR.
GDPR 前文第 25 項も参照。

73. However, the mere presence of a representative in a Member State does not trigger the one-stop-shop system[36]. For this reason the breach will need to be notified to every supervisory authority for which affected data subjects reside in their Member State. This (These) notification(s) shall be the responsibility of the controller[37].
しかしながら、加盟国の一つに代理人がいるだけでは、ワンストップショップ・システムは適用されない [36]。このため侵害は、影響を受けるデータ主体が居住する加盟国の全ての監督機関に対し通知される必要がある。この（これらの）通知は、管理者の責任である [37]。

74. Similarly, where a processor is subject to Article 3(2) GDPR, 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) GDPR.
同様に、処理者が GDPR 第 3 条(2)の対象である場合、処理者は、特にここでの関連では、GDPR 第 33 条(2)に基づく管理者に対する侵害の通知の責務という、処理者に課される義務に拘束される。

D. Conditions where notification is not required
D. 通知が要求されない場合の条件

75. Article 33(1) GDPR 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.
GDPR 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、監督機関に対する通知を要しないことを明らかにしている。個人データが既に公に利用可能であり、かつそのようなデータの開示が当該個人に対しリスクとなるおそれがない場合が一例に挙げられるであろう。これは、関連する侵害全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既存の侵害通知要件とは対照的である。

76. In its Opinion 03/2014 on breach notification[38], 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

---

[36] 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
WP29の管理者又は処理者の主監督機関を特定するためのガイドラインは、以下より入手可:
http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] In line with guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, the EDPB considers the function of a representative in the Union as not compatible with the role of an external data protection officer ("DPO"), therefore the responsibility to notify the supervisory authority in case of a personal data breach remains that of the controller in line with Article 27(5) GDPR. A representative can however be involved in the notification process if this has been explicitly stipulated in the written mandate.
GDPR の地理的適用範囲 (第 3 条) に関するガイドライン3/2018に即したもの。https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en より入手可。EDPB は、EU域内における代理人の機能が外部のデータ保護オフィサー (「DPO」) の役割とは両立しないと考えており、したがって個人データ侵害が発生した場合に監督機関に通知する責任は、GDPR 第 27 条 (5) に沿い管理者にある。ただし、書面による委任により明示的に規定されている場合には、代理人は通知の過程に関与することが可能である。

[38] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
WP29の侵害通知に関する意見03/2014: http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[39]. 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.
侵害通知に関する意見 03/2014[38] において、WP29 は、最先端技術のアルゴリズムで暗号化された個人データの機密性の侵害は依然として個人データの侵害であり、通知を要されると説明している。一方で、その鍵の機密性が損なわれていない場合、すなわち、当該鍵がいかなるセキュリティ侵害も受けておらず、かつ当該鍵にアクセス権限の無いいかなる者も現行利用可能な技術的手段により判明することが不可能であるように生成されている場合、このとき当該データは原則として識別不可能である。したがって、当該侵害は個人に対し悪影響を与えるおそれはなく、よって該当の個人に対する連絡は要されないであろう[39]。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い場合、喪失や改変によりデータ主体に対し悪影響を及ぼす可能性がある。この場合、データ自体に適切な暗号化措置が講じられていたとしても、データ主体に対する連絡は要求されよう。

77. WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.
WP29 はまた、このことは次の場合においても同様に当てはまるであろうと説明している。パスワードのような個人データが安全にソルト付与によるハッシュ化がなされており、当該ハッシュ値が最先端技術の鍵付与の暗号学的ハッシュ関数で計算され、該当のデータをハッシュ化するのに用いられた鍵がいかなる侵害も受けておらず、かつ当該データをハッシュ化するのに用いられた鍵がそれにアクセス権限の無いいかなる者も現行利用可能な技術的手段により判明することが不可能であるような方法で生成されている場合。

78. 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.
結果、個人データが無権限な者にとって実質的に識別不可能なものであり、かつ当該データがコピーであるか又はバックアップが存在する場合、適正に暗号化された個人データに関する機密性の侵害を監督機関に対し通知する必要はない。これは、そのような侵害は個人の権利と自由に対しリスクをもたらすおそれがないからである。このことは当然ながら、高いリスクをもたらすおそれがないため、該当の個人に対する連絡も必要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ならば、当初は通知が要求されないとしても、このことが時間の経過とともに変化する可能性があり、リスクを再評価する必要がありうることに留意しておかなければならない。例えば、後に鍵が侵害されていることが判明する場合、又は暗号化に使用したソフトウェアの脆弱性が露呈する場合、そのとき通知は依然要求されうる。

79. 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

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

time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) GDPR 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る場合、可用性の侵害が生じているであろうことに留意しておかなければならない。このことは個人に対しリスクをもたらすおそれがあり、結果通知が要求されうる。同様に、暗号化されたデータの喪失に関する侵害が生じる場合、たとえ個人データのバックアップが存在するとしても、そのバックアップからデータを回復するのに要する時間の長さ及びそれによる利用可能性の欠如が個人に及ぼす影響次第で、これも依然報告が要求される侵害となりうる。GDPR 第 32 条(1)(c)が定めるように、安全性の重要な要素の一つは「*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.
監督機関に対する通知が要求されないであろう侵害の一つは、管理者及びその職員の使用に供される、安全に暗号化されたモバイルデバイスの喪失であろう。使用された暗号鍵が管理者の安全な所有下にあり、かつこれが個人データの唯一のコピーではない場合、当該個人データは攻撃者にとってアクセス不可能であろう。このことは、侵害が問題のデータ主体の権利及び自由に対するリスクを生じさせるおそれがないことを意味する。後に当該暗号鍵が侵害されていた又は暗号化に使用されたソフトウェア若しくはアルゴリズムが脆弱であったことが判明する場合、自然人の権利及び自由に対するリスクは変わり、したがってそのときは通知が要求されうる。

80. However, a failure to comply with Article 33 GDPR 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中で、管理者が監督機関に対する通知をしていない場合、GDPR 第 33 条を遵守していない状況が生じる。したがって、暗号化ソフトウェアを選択するに当たり管理者は、提供される暗号化の品質及び適正な実装を慎重に検討し、それが実際に提供する保護水準の度合い及びこれが現存するリスクに対し適切か否かについて理解しておかなければならない。管理者はまた、使用する暗号化製品がどのように機能するかといった詳細に精通しておかなければならない。例えば、あるデバイスの場合、電源が切られると暗号化されるが、スタンバイモードの間は暗号化されない。暗号化を使用する製品の一部には「デフォルトキー」を有するものがあり、これを有効化するには各顧客が変更する必要がある。またセキュリティ専門家が現行適切であるとみなしうる暗号化が、数年後には時代遅れになる可能性がある。このことは、データが当該製品により十分に暗号化されているか否か、また適切な保護水準を提供し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 – データ主体に対する連絡

A. Informing individuals
A. 個人に知らせる場合について

81. In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.
一定の場合において、管理者は、監督機関に対する通知同様、影響を受ける個人に対する侵害の連絡も要求される。

Article 34(1) GDPR states:
GDPR 第 34 条(1)は次のように定めている。

> *"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おそれがある場合、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。」*

82. 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に対するリスクを発生させるおそれがない場合を除き、監督機関に対する通知が必須であることを想起しておかなければならない。加えて、侵害の結果として個人の権利及び自由に対する高いリスクを発生させるおそれがある場合、個人に対する連絡もしなければならない。個人に対し侵害を連絡する閾値は、したがって監督機関に対する通知の閾値よりも高く、全ての侵害について個人に対する連絡が要求されるわけではない。こうすることで不必要な通知疲れから個人を守っている。

83. 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[40]. 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、個人に対する侵害の連絡は「不当な遅延なく」行われなければならないと規定しており、これは可能な限り早くということを意味する。個人に対する通知の主たる目的は、個人が自身を保護するためにとるべき手立てについて特定の情報を提供することである [40]。上記の通り、侵害の性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身を保護するべく手立て講ずるのを助けることになる。

84. 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.
このガイドラインの別紙 B では、侵害が個人に対し高いリスクを生じさせるおそれがある場合の例、及びその結果管理者が影響を受ける者に対して侵害の通知を要求される場合の事例について、非網羅的なリス

[40] See also Recital 86 GDPR.
GDPR 前文第 86 項も参照。

トが提供されている。

B. Information to be provided
B. 提供する情報

85. When notifying individuals, Article 34(2) GDPR specifies that:
個人に通知する場合について、GDPR 第 34 条(2)は次のように明示している。

> *"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措置を含める。」*

86. According to this provision, the controller should at least provide the following information:
この規定に従って、管理者は少なくとも次の情報を提供しなければならない。

- a description of the nature of the breach;
- 該当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他の連絡窓口の名前及び連絡先、

- a description of the likely consequences of the breach; and
- その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.
- 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の記述。

87. 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.
侵害に対処するため、また生じうる悪影響を低減させるために講じられた措置の例として、管理者は、関連する監督機関に対し侵害を通知した後、侵害に対処し影響を低減するための助言を受けた旨を説明することが可能であろう。管理者はまた、適切な場合、個人に対し、侵害により生じうる悪影響から自身を保護するための特定の助言、例えばアクセスの認証情報が侵害されている場合のパスワードの変更といったことを提供しなければならない。ここでもまた、管理者は、要求されるものに加えて情報を提供することを選択することができる。

C. Contacting individuals
C. 個人への連絡方法について

88. 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) GDPR).
原則として、関連する侵害は、影響を受けるデータ主体に対して直接連絡されなければならない。ただし、過大な負担を要する場合は除外される。そのような場合、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(GDPR 第 34 条(3)(c))。

89. 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.
データ主体に対し侵害を連絡する場合、侵害だけに特化した通信文を使用しなければならず、また当該通信文は、例えば定期的なアップデート、ニュースレター又は標準メッセージのようなその他の情報と一緒に送信してはならない。このことにより、侵害についての連絡が明確かつ透明性のあるものとなる。

90. 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. The EDPB recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.
透明性のある連絡の方法の例は、直接的な連絡（例えば、電子メール、ショートメッセージサービス、ダイレクトメッセージ）、人目を引くウェブサイトのバナー又はお知らせ、郵送による連絡、及び新聞媒体での人目を引く広告を含む。プレスリリース又は企業ブログ内のみに限定された通知は、個人に対し侵害を連絡する手段として効果的ではないであろう。EDPB は、管理者が影響を受ける全ての個人に対し適切に情報を連絡する機会を最大化するような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、複数の連絡方法を採用することを意味することがありうる。

91. 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、個人が自身に提供される情報を理解できるよう確保するため、当該連絡が適切な代替的形式及び該当する言語でアクセスできるよう確保する必要がありうる。例えば、個人に対する侵害を連絡する場合、使用する言語は、当該連絡の受け手側と以前に通常業務過程で使用したものが一般的には適切であろう。しかしながら、以前に管理者が接触したことのないデータ主体、又は特に管理者が拠点とする国とは異なる加盟国若しくは他の EU 域外国に居住するデータ主体に対し、侵害が影響を与える場合、必要とされるリソースを考慮したうえで、該当する国の母国語で連絡することが適切である場合がある。重要なのは、データ主体が侵害の性質及び自身を保護するために講ずることのできる手立てを理解するよう手助けすることである。

92. 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、特に頻繁に自身の顧客と接触している場合、個人に対し侵害を連絡するための最も適切な連絡経路を判断する最適な立場にある。一方、明らかに管理者は、侵害により不正アクセスされた連絡経路

の使用について注意しなければならない。このような連絡経路は、管理者になりすました攻撃者にも使用される可能性があるからである。

93. At the same time, Recital 86 GDPR explains that:
同時に、GDPR 前文第 86 項は次のように説明している。

> *"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。」*

94. 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.
したがって、管理者は、第 34 条に従い侵害についてデータ主体に知らせるかどうかについて助言を求めるためだけではなく、個人に対し送信すべき適切なメッセージ及び個人に接触する最も適切な方法についても監督機関に連絡し協議することを希望するかもしれない。

95. Linked to this is the advice given in Recital 88 GDPR 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 GDPR 前文第 88 項に定められている助言であり、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に入れ」なければならない、というものである。このことは、一定の状況下であり、正当な理由があり、かつ法執行機関の助言に基づいて、管理者は、連絡がそのような捜査を妨げるようなことがなくなるまでの間、影響を受ける個人に対する侵害の連絡を遅らせることができることを意味しうる。ただし、データ主体は、依然、この後速やかに連絡を受ける必要があろう。

96. 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).
ある個人に連絡するために保存されていたデータが十分ではなく、管理者が当該個人に対し侵害の連絡をすることができない場合、そのような特定の状況において管理者は、侵害の連絡が合理的に実行可能になり次第すぐに当該個人に連絡しなければならない（例えば、ある個人が個人データにアクセスするための第 15 条の権利を行使し、管理者に対し連絡に必要な追加的情報を提供する場合）。

D. Conditions where communication is not required
D. 連絡が要求されない場合の条件

97. Article 34(3) GDPR states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:
GDPR 第 34 条(3)は、侵害が生じた場合、もし満たされれば、個人に対する通知を要しないとする三つの条件について定めている。これらは次のものである。

- 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、侵害が生じる以前に個人データを保護するための適切な技術的及び組織的措置、特に、アクセス権限の無い者に対し個人データを識別不可能にするような措置が講じられていた場合。これには、例えば、最先端的技術による暗号化、又はトークン化を用いた個人データの保護が含まれうるであろう。

- 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具体化しないようにすることを確保する手立てを講じていた場合。例えば、事案の状況によっては、管理者は、個人データにアクセスした者が個人データを使用し何らできるようになる前に、その者を直ちに特定し、その者に対し措置を講じうる。ここでも、関係するデータの性質に応じて、あらゆる機密性の侵害により生じうる結果について十分に考慮することが、依然、要される。

- It would involve disproportionate effort[41] 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.
- 恐らく、侵害の結果個人の連絡先が失われた場合又はそもそも知らない場合、個人に連絡するために過大な負担 [41] を要するであろう。例えば、統計当局の倉庫が洪水に見舞われ、個人データを含んだ文書が紙ベースでのみ保管されていた場合である。代わりに、個人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。過大な負担を要する場合に備えて、侵害についての情報を要求に応じて利用可能にする技術的な措置を講じておくことも想定されうるであろう。このことは、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連絡することができない個人にとって有用なものとなりうるであろう。

98. In accordance with the accountability principle controllers should be able to demonstrate to the supervisory

[41] 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
過大な負担の問題について検討している、WP29 の透明性についてのガイドラインを参照。以下より入手可: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

authority that they meet one or more of these conditions[42]. 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の原則に従い、管理者は、監督機関に対し、これらの条件のうち 1 つ以上を充足していることを証明できるようにしなければならない[42]。個人の権利と自由に対するリスクのおそれがないならば、当初は通知が要求されないとしても、このことが時間の経過とともに変化する可能性があり、リスクを再評価する必要がありうることに留意しておかなければならない。

99. If a controller decides not to communicate a breach to the individual, Article 34(4) GDPR 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) GDPR 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.

管理者が個人に対する侵害の連絡をしないという決定をする場合でも、GDPR 第 34 条(4)は、侵害が個人に対し高いリスクを発生させるおそれがあると判断する場合、監督機関は、管理者に対しそのようにするよう要求できると説明している。あるいは、監督機関は、個人への通知が要求されない GDPR 第 34 条(3)に定める要件が満たされていると判断するかもしれない。データ主体への通知をしないという決定が十分に根拠のあるものではないと判断する場合、監督機関は、利用可能な権限と制裁の行使を検討する可能性がある。

IV. ASSESSING RISK AND HIGH RISK
IV. リスク及び高いリスクの評価

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

100. Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:
GDPR は侵害を通知する義務を導入しているものの、全ての状況において通知することを要件とし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に対するリスクを発生させるおそれがない場合を除き、所轄監督機関に対する通知が要求される。

- 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対する高いリスクを発生させるおそれがある場合のみ、その個人に対する侵害の連絡が要求される。

101. 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,

[42] See Article 5(2) GDPR.
GDPR 第 5 条(2)参照。

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、侵害を認識した時点で直ちに、管理者は、侵害の阻止を追求するだけでなく、その侵害から発生しうるリスクを評価することが極めて重要であることを意味する。これには 2 つの重要な理由がある。第一に、個人に対する影響の蓋然性及び潜在的深刻度を知ることで、管理者は、その侵害を阻止し対応するための実効的手立てを講ずることができるようになる。第二に、それは、監督機関に対する通知が要求されるか否か、また必要に応じて、関係する個人に対する通知が要求されるか否かについて管理者が判断するのを助ける。

102. 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[43].
前述のとおり、侵害の通知は、個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要求され、データ主体に対する侵害の連絡が要求される発動条件の要は、個人の権利及び自由に対する*高い*リスクを発生させるおそれがある場合である。このリスクは、侵害が、そのデータが侵害された個人にとって物的な損失、財産的な損失又は非財産的な損失を発生させうる場合に存在する。このような損失の例として、差別、ID 盗取又は ID 詐欺、金銭上の損失及び信用の棄損がある。侵害が、人種的若しくは民族的な出自、政治的な意見、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生活と関連するデータ、又は有罪判決及び犯罪行為若しくは関連する保護措置と関係するデータを含む場合、このような損失が生じるおそれがあると判断されうるであろう[43]。

B. Factors to consider when assessing risk
B. リスク評価に当たって考慮する要素

103. 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、一般にリスクを評価する際、データ主体の権利及び自由に対するリスクの蓋然性及び深刻度の両方を考慮するよう提言している。さらに、リスクは客観的な評価に基づいて決定されなければならないと定めている。

104. 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[)][44]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.
侵害の結果として生じる人々の権利及び自由に対するリスクを評価する場合、DPIA の中で考慮されるリス

[43] See Recital 75 and Recital 85 GDPR.
GDPR 前文第 75 項及び前文第 85 項参照。

[44] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
WP29 の DPIA に関するガイドライン、以下、参照：http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

クとは異なる焦点を有するということに留意しなければならない [44]。DPIA は、データ取扱いが計画の通り実施されることのリスク、及び侵害が生じた場合のリスクの両方を考慮している。潜在的な侵害を考慮する場合、一般的に侵害が発生する蓋然性、及びその結果として生じうるデータ主体に対する損失を考察する。言い換えれば、これは仮定的な事象の評価である。実際の侵害の場合、事象は既に発生しているため、焦点はもっぱら侵害が個人に及ぼす影響から生じるリスクに当てられることになる。

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ために、ある特定のセキュリティソフトウェア製品を利用する提案が適切な措置であることを示している。当該措置は、それがない場合に取扱いが個人にもたらすであろうリスクに対し、適切に一定のレベルの安全性を確保するものである。一方、その後に何らかの脆弱性が明らかとなる場合、このことにより保護対象の個人データに対するリスクを阻止する目的のための当該ソフトウェアの適切性が変わるかもしれない。したがって、継続的に実施する DPIA の一環として当該措置を再評価する必要があろう。

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.

当該製品の脆弱性が後に利用され、侵害が発生する。管理者は、当該侵害の特定の状況、影響を受けるデータ、個人への潜在的な影響のレベル、及び当該リスクが実現するであろう蓋然性について評価しなければならない。

105. Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. The EDPB therefore recommends the assessment should take into account the following criteria[45]:

したがって、侵害の結果としての個人に対するリスクを評価する際、管理者は、潜在的な影響の深刻度及びその蓋然性を含む、侵害の特定の状況を考慮しなければならない。よって、EDPB は、リスク評価には次の事項を考慮に入れるよう勧告する [45]。

- **The type of breach**
- **侵害の種類**

106. 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、個人に対しもたらすリスクレベルに影響する場合がある。例えば、医療情報が無権限の者に開示されるといった機密性の侵害は、ある個人の医療情報の詳細を喪失し、利用不能となる

[45] 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 3.2 条は、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素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りうる。以下参照：http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

場合の侵害とは異なる結果を個人にもたらしうる。

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

107. 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、リスク評価をする際、主要な要素は侵害により不正アクセスされた個人データの種類及び機微性である。通常、データの機微性が高まるほど、影響を受ける人々に危害が及ぶリスクも高まる。一方、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しなければならない。例えば、通常の状況において個人の氏名及び住所の開示が重大な損失の原因となるおそれはない。一方、ある養育者の氏名及び住所が産みの親に開示される場合、その結果が当該養育者及び子どもの両者にとって極めて深刻なものとなる可能性がある。

108. 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.
健康に関するデータ、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に関する侵害は、全てそれ自体で危害を生じうるが、併せて使用される場合、ID 盗取に使用される可能性がある。一般に、個人データの組合せは、単一の個人データよりも機微性が高い。

109. 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.
一部の種類の個人データは、当初は比較的無害に見えるかもしれない。一方、当該データが、影響を受ける個人についての何を明らかにするかについて、慎重に検討する必要がある。定期配達を受入れている顧客のリストは特段、機微性はないかもしれないが、休日の配達の停止を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。

110. 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、少量だが機微性の高い個人データは、個人に対して高い影響を及ぼしうる。また、広範囲にわたる詳細情報は、その個人についてより広い範囲の情報を明らかにしうる。加えて、多数のデータ主体についての莫大な量の個人データに影響を及ぼす侵害は、対応する多数の個人に影響を及ぼす可能性がある。

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

111. 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素の一つは、侵害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すること、又は当該データと他の情報とを照合して個人を特定することがどの程度容易かということである。状況によっては、個人の身元を判明するために特別な調査を必要とせず、侵害された個人データから直接身元を特定することが可能な場合があろう。又は、個人データをある特定の個人に照合するのが極めて困難でありうるが、一定の条件下では依然可能な場合がある。身元の特定は侵害されたデータから直接的又は間接的に可能でありうるが、それはまた、侵害の特定の状況及び関連する個人情報が公に利用可能なものかにも依存する。これは機密性及び可用性の侵害に、より関係しうる。

112. 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) GDPR 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、適切なレベルの暗号化により保護された個人データは、復号鍵を持たない無権限の者にとって識別不可能である。加えて、適切に実装された仮名化（GDPR 第 4 条(5)において「*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*」と定義されている）もまた、侵害が発生した場合に個人の身元が特定される蓋然性を低減しうる。ただし、仮名化技術だけではデータを識別不可能とするものとはみなされない。

- **Severity of consequences for individuals**
- **個人にとっての結果の深刻度**

113. 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.
例えば、特別な種類のデータといった、侵害に関与する個人データの性質に応じて、発生する可能性のある個人に対する潜在的な損失は特に深刻なものとなりうる。特に、侵害が ID 盗取又は ID 詐欺、身体的危害、心理的苦痛、侮辱又は信用の毀損を生じさせる可能性がある場合である。侵害が脆弱性のある個人についての個人データに関する場合、これらの個人はより大きな危害のリスクにさらされる可能性がある。

114. 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).
個人データが意図の不明な者又は悪意を持っている可能性のある者の手に渡っているということを管理者が認識しているか否かは、潜在的なリスクレベルに影響を及ぼしうる。個人データが、第 4 条(10)に定義する第三者に対し、又は誤ってその他の取得者に対し開示される場合、機密性の侵害が生じうる。これは、例えば、個人データが、同じ組織の間違った部門に、又は通常使用しているサプライヤーの組織に対し、偶発的に送信される場合に起こりうる。管理者は、取得者に対して、受領したデータを返却するよう又は安全に破棄するよう要求しうる。いずれの場合も、管理者が当該取得者と継続的な関係を有しており、また管理者が当該取得者の作業手順、経歴及びその他の関連詳細情報を認識しうるとすれば、当該取得者は「信用できる」とみなされうる。言い換えれば、管理者は当該取得者について、誤って送信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ということを合理的に期待することができるような一定レベルの確証を有しうるということである。データにアクセスされた場合でも、管理者は依然、取得者がそれを使用して追加的な行動をとることがないこと、また直ちに管理者に対しデータを返却し、その回復に協力してくれることを信用できる可能性があろう。このような場合、管理者は、侵害に続いて実施するリスク評価に、このことを要素として組み込みうる。取得者が信頼されているという事実は、侵害の結果の深刻度を取り除きうるが、侵害が発生しなかったことを意味するわけではない。一方、このことにより個人に対するリスクの可能性が取り除かれ、結果、監督機関又は影響される個人に対する通知が要求されなくなる可能性がある。繰り返しになるが、これはケースごとに異なる。それでも依然、管理者は、侵害の記録を維持するという一般的義務の一部として、当該侵害に関する情報を保管しなければならない（下記、第 V 章を参照）。

115. 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.
もし侵害の影響が長期間となり、個人への影響がより大きくなるとみなされうる場合、個人に対する影響の永続性についても考慮しなければならない。

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

116. 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、子どものほか脆弱性のある者に関する個人データに対して影響を与える可能性がある。こういった個人は、より大きな危害のリスクにさらされうる。侵害の影響レベルに作用しうるような、こういった個人に関する他の要素もあるかもしれない。

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

117. 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レベルに影響しうる。

例えば、医療機関は、特別な種類の個人データを取り扱うであろう。このことは、その個人データが侵害される場合、新聞の郵送リストの場合に比し、個人にとってより大きな脅威があることを意味する。

- **The number of affected individuals**
- **影響を受ける個人の数**

118. 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 名のみ若しくは数名の個人、又はそれ以上ではないとしても数千名に影響しうる。一般に、影響を受ける個人の数が多いほど、侵害の影響は大きくなりうる。一方、個人データの性質及びそれが侵害された過程次第では、侵害はたとえ 1 名の個人に対しても深刻な影響を与える可能性がある。ここでもまた、肝要なのは、当該影響を受ける者に対する影響の蓋然性及び深刻度を考慮することである。

- **General points**
- **一般的な点**

119. 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、侵害から生じるおそれのあるリスクを評価する際、管理者は、個人の権利及び自由に対する潜在的な影響の深刻度、及びこれらが発生する蓋然性の組合わせを考慮しなければならない。明らかに、侵害の結果がより深刻な場合、リスクはより高くなる。同様に、これらが発生する蓋然性が高ければ、リスクもまた高くなる。疑わしい場合、管理者は、過剰なほど注意を払い、通知をしなければならない。別紙 B では、個人に対するリスク又は高いリスクを伴う様々な種類の侵害についての有用な事例が提供されている。

120. 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[46].
欧州ネットワーク・情報セキュリティ機関（ENISA）は、管理者及び処理者がその侵害管理対応計画を策定する際に役立つであろう、侵害の深刻度を評価する方法についての勧告を作成している [46]。

V. ACCOUNTABILITY AND RECORD KEEPING
V. アカウンタビリティ及び記録の保管

A. Documenting breaches
A. 侵害の文書化

121. 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) GDPR explains:

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

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、GDPR 第 33 条(5)が説明するとおり、全ての侵害を文書化したもの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。」*

122. This is linked to the accountability principle of the GDPR, contained in Article 5(2) GDPR. The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24 GDPR, 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[47].
これは GDPR 第 5 条(2)に含まれている、GDPR のアカウンタビリティの原則に関連している。通知が要されない侵害を記録する目的は、通知が要される侵害の場合と同様、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。したがって管理者は、通知の要否にかかわらず、侵害についての内部的な登録を確立しておくことが推奨される [47]。

123. 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) GDPR, 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.
侵害を文書化する際、どのような方法及び構成を使用するかについて判断するのは管理者の責任であるが、記録が要される情報については、全ての場合において含めなければならない主要な要素がある。GDPR 第 33 条(5)で求められているように、管理者は侵害に関する詳細情報を記録する必要があり、それには侵害の原因、発生した事態及び影響を受けた個人データが含まれる。加えて、侵害の影響及び結果、並びに管理者により講じられた救済措置も含めなければならない。

124. 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[48] and to meet a lawful basis for processing[49]. It will need to retain documentation in accordance with Article 33(5) GDPR 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[50] of the GDPR does not apply.

---

[47] The controller may choose to document breaches as part of [if] its record of processing activities which is maintained pursuant to Article 30 GDPR. 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 条に従い保管される取扱い活動の記録の一部として侵害を文書化しておくことを選びうる。独立して登録しておくことは要求されていないが、このとき、侵害に関連する情報が明確にそれであると特定可能であること、また要求に応じて取り出すことが可能であることが前提となる。

[48] See Article 5 GDPR.
GDPR 第 5 条参照。

[49] See Article 6 and also Article 9 GDPR.
GDPR 第 6 条及び第 9 条も参照。

[50] See Article 5(1)(e) GDPR.
GDPR 第 5 条(1)(e)参照。

GDPR はこれらの文書の保存期間を明示していない。このような記録が個人データを含む場合、個人データの取扱いに関する基本原則に従い適切な保存期間を判断し[48]、また取扱いの適法性を満たす[49]ことは、管理者の責務である。GDPR 第 33 条(5)の遵守、より一般的にはアカウンタビリティの原則の遵守の証拠を監督機関に対し提供するよう求められる可能性があるため、同条に従い文書を保管しておく必要がある。記録内に個人データが含まれていない場合、明らかに、GDPR の記録保存の制限の原則[50]は適用されない。

125. In addition to these details, the EDPB 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[51]. Alternatively, if the controller considers that any of the conditions in Article 34(3) GDPR 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、EDPB は、管理者が侵害に対応するために行った決定の根拠についても文書化しておくよう勧告する。特に、侵害の通知をしない場合、当該決定を正当化する根拠を文書化しておかなければならない。これには、管理者が、その侵害が個人の権利及び自由へのリスクを発生させるおそれがないとみなす理由を含めなければならない[51]。一方、GDPR 第 34 条(3)のいずれかの条件が満たされているとみなす場合、管理者は、条件を満たしているという適切な証拠を提出できるようにしておかなければならない。

126. 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対し、侵害の通知自体はしているが、その通知が遅滞している場合、管理者はその遅延の理由を提出できなければならない。これに関して文書化しておくことは、その報告の遅延が正当なものであり、過度なものではないということを証明するのに役立つ可能性がある。

127. 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.
管理者が影響を受ける個人に対し侵害を連絡する場合、侵害について透明性があり、また効果的かつ適時な方法で連絡しなければならない。したがって、そのような連絡の証拠を保管しておくことは、管理者がアカウンタビリティ及び遵守を証明するために役立つであろう。

128. To aid compliance with Articles 33 and 34 GDPR, 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.
GDPR 第 33 条及び第 44 条の遵守を支援するために、侵害の検知に続く作業、つまりインシデントの阻止、制御、及び復旧の方法、リスク評価の方法、並びに侵害通知の方法を定めた、通知の手順書を文書化して整備しておくことは、管理者及び処理者の両方にとって有益であろう。この点について、GDPR の遵守を示すために、従業員がこれらの手順書及び仕組みの存在について知らされていること、また従業員が侵害への対処方法を知っていることを証明することもまた有用であろう。

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

[51] See Recital 85 GDPR.
GDPR 前文第 85 項参照。

Article 83 GDPR.
侵害を適切に文書化しない場合、監督機関が GDPR 第 58 条に基づき権限を行使し、及び／又は、GDPR 第 83 条に基づき制裁金を科すことにつながる可能性があることに留意しなければならない。

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

130. A controller or processor may have a Data Protection Officer (DPO)[52], either as required by Article 37 GDPR, 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、GDPR 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）を置く場合がある [52]。GDPR 第 39 条は、DPO の一連の必須の職務を定めているが、適切な場合、管理者が追加的な職務を担当させることを妨げていない。

131. 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) GDPR requires the controller to provide the name and contact details of its DPO, or other contact point.
このうち特に侵害通知に関連するものとして、DPO の必須の職務には、中でも、管理者又は処理者に対するデータ保護に関する助言及び情報の提供、GDPR への遵守の監視、並びにデータ保護影響評価に関する助言の提供がある。DPO はまた、監督機関と協力し、監督機関及びデータ主体の連絡窓口として行動しなければならない。加えて、監督機関に対し侵害を通知する際、GDPR 第 33 条(3)(b)は、管理者が DPO の氏名及び連絡先、又は他の連絡窓口を提供するよう要件としていることに留意しなければならない。

132. 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、当該文書の構成、設定及び管理について DPO の意見を得ることを希望する場合がある。加えて DPO は、そのような記録の保管についても担当する場合もあろう。

133. These factors mean that the DPO should play a[n] 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, the EDPB recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.
これらの要素は、DPO が、助言の提供及びコンプライアンスの監視による侵害の阻止又は侵害に対する事前の準備への支援において、侵害が発生している間（すなわち、監督機関への通知の際）において、また事後の監督機関による調査の実施中において、主要な役割を果たすであろうことを意味する。この観点から、EDPB 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プロセスの全体にわたり関与していくよう勧告する。

VI. NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS
VI. 他の法令に基づく通知義務

[52] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
WP29 の DPO についてのガイドライン参照: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

134. 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 に基づく侵害の通知及び連絡に加え、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令に基づくセキュリティインシデントのあらゆる通知要件について、また、これが同時に、監督機関に対する個人データ侵害の通知を管理者に要求しているか否かについて認識しておかなければならない。このような要件は加盟国間で異なりうるが、他の法令における通知要件の例、及びどのようにこれらの通知要件が GDPR と相互に関係しているかについては、次のようなものがある。

- *Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*[53].
- *域内市場における電子取引のための電子識別及びトラストサービスに関する規則(EU)910/2014(eIDAS 規則)*[53]。

135. Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.
eIDAS 規則の第 19 条(2)は、提供したトラストサービスに対し又はその際に保管された個人データに対し深刻な影響を及ぼすセキュリティ侵害又は完全性の喪失が生じる場合、トラストサービスのプロバイダーは、自らの監督組織に対し通知するよう要求している。該当する場合、すなわち、そのような侵害又は喪失が GDPR に基づく個人データ侵害でもある場合、当該トラストサービスのプロバイダーはまた、該当の監督機関に対し通知しなければならない。

- *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*[54].
- *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)*[54].

136. 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[55], 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、基幹サービス運営者及びデジタルサービスプロバイダーがその所轄官庁に対し、セキュリティインシデントの通知をするよう要求している。NIS 前文第 63 項において認識されてい

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

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

[55] 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:*「インシデントの結果として多くの場合、個人データが侵害される。この文脈において、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あらゆる個人データ侵害に対応するため、全ての関連事項について協力し、また情報交換をしなければならない。」*

るように [55]、セキュリティインシデントは個人データの侵害を含みうることが多い。その文脈において、NIS は、所轄官庁及び監督機関に対し、関連事項について協力し情報交換するよう要求している。一方、このようなインシデントが GDPR に基づく個人データ侵害である又はそうなる場合、運営者及び／又はプロバイダーは、NIS の要件であるインシデントの通知とは別に、該当の監督機関に対する通知が要求されることに変わりはない。

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 指令に基づき侵害の通知を行うクラウドサービスプロバイダーは、当該侵害が個人データ侵害を含む場合、管理者に対する通知も要求されうる。同様に、eIDAS に基づき通知を行うトラストサービスプロバイダーは、侵害が生じた場合、関連するデータ保護機関に対する通知も要求されうる。

- *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）及び規則 611/2013（侵害通知規則）*

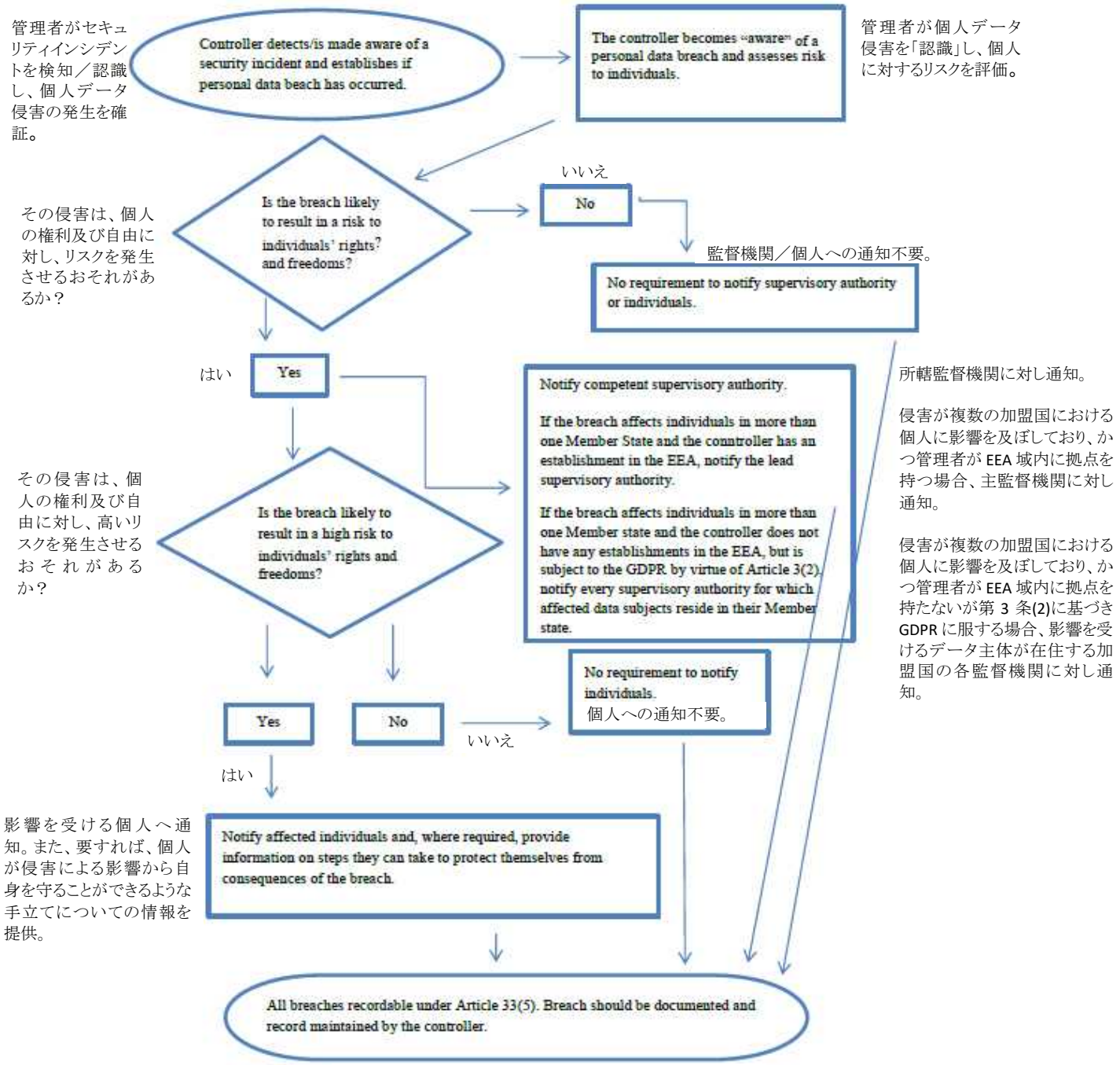
137. Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[56] must notify breaches to the competent national authorities.
指令 2002/58/EC[56] の適用範囲内で、公衆に利用可能な電子通信サービスのプロバイダーは、国内の所轄官庁に対し侵害を通知しなければならない。

138. Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.
管理者はまた、他の適用される制度に基づく追加的な法律上、医療上又は職務上の通知義務について認識しておかなければならない。

[56] 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-electroniccommunications
2017 年 1 月 10 日、欧州委員会は、プライバシー及び電子通信に関する規則を提案した。これは、指令 2009/136/EC に置き換わり、また、通知要件が取り除かれる予定のものである。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

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



B. Examples of personal data breaches and who to notify
B. 個人データ侵害及び通知先の事例

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.
次の事例は全てを網羅するものではないが、管理者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。これらの事例はまた、個人の権利及び自由に対するリスクと高いリスクとを区別する手助けにもなりうる。

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.管理者は、個人データのアーカイブのバックアップをUSB キー上に暗号化し保管している。休憩中に当該キーが盗まれる。	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. データが最先端技術のアルゴリズムで暗号化されており、データのバックアップが存在し、一意の鍵が侵害されておらず、かつデータが適時に復元可能である限り、これは報告対象となる侵害ではない。但し、後に侵害が生じる場合、通知が要求される。
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維持管理している。当該サービスへのサイバー攻撃の結果、各人の個人データが流出する。 管理者は、単一の加盟国に顧客を有する。	Yes, report to the supervisory authority if there are likely consequences to individuals. はい。個人に影響するおそれがある場合、監督機関に報告する。	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。影響を受ける個人データの性質に応じて、また個人に対し生じうる結果の深刻度が高い場合、個人に報告する。	
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.	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.

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により、顧客は管理者に連絡できず、自らの記録にアクセス不能となる。			これは通知対象となる侵害ではないが、依然第 33 条(5)に従い記録対象となるインシデントである。 管理者は適切な記録を保管すること。
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.管理者がランサムウェア攻撃を受け、その結果全データが暗号化される。利用可能なバックアップはなく、データを復元することができない。調査において、ランサムウェアの唯一の機能はデータの暗号化であり、システム内に他のマルウェアは存在しないことが明らかとなる。	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability. はい。これは可用性の喪失であり、個人に対する影響のおそれがある場合、監督機関に報告する。	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。影響を受ける個人データの性質、データの可用性の欠如から生じうる影響及びその他の生じうる影響に応じて、個人に報告する。	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. 利用可能なバックアップがあり、適時にデータが復元可能な場合、可用性又は機密性の恒久的な喪失は生じないであろうから、監督機関に対する、又は個人に対する報告は要されないであろう。ただし、監督機関が他の手段によるインシデントを認識するに至る場合、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、調査を考慮しうる。
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.ある個人が銀行のコールセンターに電話し、データ侵害を報告する。当該個人は別人の月次明細書を受領していた。 管理者は、短時間の調査(すなわち 24 時間以内に完了するもの)を実施し、個人	Yes. はい。	Only the individuals affected are notified if there is high risk and it is clear that others were not affected. 高いリスクがあり、かつ他に影響を受けている者がいないことが明らかな場合、影響を受ける個人に対してのみ通知する。	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. 追加的な調査の結果、より多くの個人が影響を受けていることが判明する場合、監督機関に対し最新情報を提供しなければならず、また管理者は、他の個人に対しても高いリスクが生じる場合、当該個人に対し通知するという追加的手立てを講ずること。

データ侵害が生じていること、また他の個人も影響を受けている又は受ける可能性のあるシステム上の欠陥が存在しているか否かを、合理的な確信をもって確認する。			
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ており、複数の加盟国に顧客を有している。当該マーケットプレイスがサイバー攻撃を受け、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上に公表される。	Yes, report to lead supervisory authority if involves cross-border processing. はい。越境取扱いが関わる場合、主監督機関に報告する。	Yes, as could lead to high risk. はい。高いリスクにつながるおそれがあるため。	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、影響を受けたアカウントのパスワードの強制リセットの他、リスクを低減するための手立て等の措置を講じなければならない。 管理者はまた、デジタルサービスプロバイダーとしての NIS 指令に基づく通知義務等、他のあらゆる通知義務も考慮しなければならない。
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の役割を担うウェブサイトホスティング会社が、ユーザー認証を制御するコードにエラーを特定する。この欠陥の影響は、いずれのユーザーも、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ものである。	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、不当な遅滞なく、影響を受ける依頼人（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独自の調査を実施したと仮定すると、ホスティング会社（処理者）から通知を受けた時点で、影響を受	If there is likely no high risk to the individuals they do not need to be notified. 個人に対する高い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、他のあらゆる通知義務について考慮しなければならない（例えば、デジタルサービスプロバイダーとしての NIS 指令に基づく通知義務）。 該当の脆弱性がいずれの管理者についても悪用されたという証拠がない場合、通知対象の侵害は起きていないが、記録対象になるか、さもなくば第 32 条に基づく遵守違反の問題となる可能性がある。

	ける管理者は、それぞれが侵害を受けたか否かの合理的な確信があるはずであり、したがって「認識した」とみなされる可能性が高い。このとき管理者は、監督機関に対する通知を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 時間利用不能となる。	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur. はい。患者の健康及びプライバシーに高いリスクが生じうるため、病院は通知する義務を負う。	Yes, report to the affected individuals. はい。影響を受ける個人に報告する。	
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、受信者が 1000 人を超える間違ったメーリングリストに、誤って送信される。	Yes, report to supervisory authority. はい。監督機関に対し報告する。	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences. はい。関与する個人データの規模及び種類、並びに生じうる結果の深刻度に応じて、個人に報告する。	
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.あるダイレクトマーケティングの電子メールが「to:」又は「cc:」フィールドの受信者に送信され、こ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る。	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。多数の個人が影響を受ける場合、センシティブデータが明らかになる場合（例えば、心理療法士のメーリングリスト）、又は他の要素が高いリスクを示す場合（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。関与する個人データの規模及び種類、並びに生じうる結果の深刻度に応じて、個人に報告する。	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、かつ少数の電子メールアドレスのみが明らかにされる場合、通知は必要ない。