仮日本語訳

Guidelines 01/2021 on Examples regarding Personal Data Breach Notification
個人データ侵害通知の事例に関するガイドライン 01/2021

Adopted on 14 December 2021
2021 年 12 月 14 日採択
Version 2.0
バージョン 2.0

本書面は、The European Data Protection Board（欧州データ保護会議）により 2021 年 12 月 14 日に採択された“Guidelines 01/2021 on Examples regarding Personal Data Breach Notification” 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 2.0 バージョン 2.0	14 12 2021 2021 年 12 月 14 日	Adoption of the Guidelines after public consultation 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
Version 1.0 バージョン 1.0	14 01 2021 2021 年 1 月 14 日	Adoption of the Guidelines for public consultation パブリック・コンサルテーションのため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 (1e) 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 Communication from the Commission to the European Parliament and the Council titled Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation[2],
欧州委員会から欧州議会及び理事会に対する報告書「市民の権限強化及びデジタル化への EU の取組みの一つの柱としてのデータ保護―一般データ保護規則の適用から 2 年」[2]に鑑み、

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

1 INTRODUCTION
1 はじめに

1. The GDPR introduces, in certain cases, the requirement for a personal data breach to be notified to the competent national supervisory authority (hereinafter "SA") and to communicate the breach to the individuals whose personal data have been affected by the breach (Articles 33 and 34).
   GDPR は、一定のケースにおいて、国内の所轄監督機関（以下「SA」という）に対する個人データ侵害の通知、及び、その侵害の影響を受けているデータ主体に対する個人データ侵害の連絡の要件を導入している（GDPR 第 33 条、34 条）。

2. The Article 29 Working Party already produced a *general* guidance on data breach notification in October 2017, analysing the relevant Sections of the GDPR (Guidelines on Personal data breach notification under Regulation 2016/679, WP 250) (hereinafter

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
本ガイドライン中の「加盟国」という表現は、「EEA 加盟国」と解釈されたい。
[2] COM(2020) 264 final, 24 June 2020.
2020 年 6 月 24 日 COM(2020) 264 最終版。

"Guidelines WP250)[3]. However, due to its nature and timing, this guideline did not address all practical issues in sufficient detail. Therefore, the need has arisen for a *practice-oriented, case-based* guidance, that utilizes the experiences gained by SAs since the GDPR is applicable.

第 29 条作業部会は GDPR の関連条項を分析し、2017 年 10 月に、データ侵害通知に関する*一般的なガイダンス*（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）（以下「ガイドライン WP250」という）[3]を既に作成しているが、その性質及びタイミングから、当該ガイドラインは全ての実務的な問題に十分詳細に対応するものではなかった。そのため、GDPR が適用されてから SA が得た経験を活用した、*実務重視の、事例に基づく*ガイダンスの必要性が生じている。

3. This document is intended to complement the Guidelines WP 250 and it reflects the common experiences of the SAs of the EEA since the GDPR became applicable. Its aim is to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment.

本ガイドラインは、ガイドライン WP 250 の補足を意図するものであり、GDPR の適用開始以来の EEA の SA の共通経験を反映している。その目的は、データ侵害をどのように取扱い、リスク評価においてどの要素を考慮すべきかについてデータ管理者の決定を助けることである。

4. As part of any attempt to address a breach the controller and processor should first be able to recognize one. The GDPR defines a "personal data breach" in Article 4(12) as "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".

侵害対応の試みの一環として、管理者及び処理者はまず、侵害を認識できなければならない。GDPR は第 4 条第 12 項において「個人データ侵害」を「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」と定義している。

5. In its Opinion 03/2014 on breach notification[4] and in its Guidelines WP 250, WP29 explained that breaches can be categorised according to the following three well-known information security principles:

第 29 条作業部会は、侵害通知に関する意見書 03/2014[4]及びガイドライン WP250 において、侵害は広く認知されている以下の三つの情報セキュリティ原則に基づき分類することができると説明している。

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.

[3] G29 WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 - endorsed by the EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
第 29 条作業部会、「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.1、2018 年 2 月 6 日、EDPB（欧州データ保護会議）承認版、https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[4] G29 WP213, 25 March 2014, Opinion 03/2014 on Personal Data Breach Notification, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.
第 29 条作業部会、「個人データ侵害通知に関する意見書 03/2014」、WP213、2014 年 3 月 25 日、P5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

「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。
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.[5]
  「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の喪失又は破壊がある場合。[5]

6. 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. One of the most important obligation of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them.
   侵害は、物的な損失、財産的な損失又は非財産的な損失をもたらしうるような、個人に対する様々な範囲の重大な悪影響を及ぼす可能性がある。GDPR は、これには、個人データに対する管理の欠落、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、及び職務上の守秘義務によって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している。また、その個人に対するそれら以外の重大な経済的又は社会的な不利益も含まれる場合がある。データ管理者の最も重要な義務の一つは、データ主体の権利及び自由に対するこれらのリスクを評定し、それらに対応するための適切な技術上及び組織上の措置を実装することである。

7. Accordingly, the GDPR requires the controller to:
   そのため、GDPR は、管理者に対し次のことを要求している。

   - document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken[6];
     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すること[6]。
   - notify the personal data breach to the supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons[7];
     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、監督機関に対し、その個人データ侵害を通知すること[7]。
   - communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural

[5] See Guidelines WP 250, p. 7. - It must be taken into consideration that a data breach can concern either one category or more categories simultaneously or combined.
ガイドライン WP250、P7、参照。データ侵害は 1 つの種類、又は同時に若しくは複合的に複数の種類に関わる場合があることを考慮しなければならない。

[6] GDPR Article 33(5). GDPR 第 33 条第 5 項

[7] GDPR Article 33(1). GDPR 第 33 条第 1 項

persons[8].
個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、そのデータ主体に対し、その個人データ侵害を連絡すること[8]。

8. Data breaches are problems in and of themselves, but they may be also symptoms of a vulnerable, possibly outdated data security regime, they may also indicate system weaknesses to be addressed. As a general truth, it is always better to prevent data breaches by preparing in advance, since several consequences of them are by nature irreversible. Before a controller can*fully* assess the risk arising from a breach caused by some form of attack, the root cause of the issue should be identified, in order to identify whether any vulnerabilities that gave rise to the incident are still present, and are still therefore exploitable. In many cases the controller is able to identify that the incident is likely to result in a risk, and is therefore to be notified. In other cases the notification does not need to be postponed until the risk and impact surrounding the breach has been fully assessed, since the full risk assessment can happen in parallel to notification, and the information thus gained may be provided to the SA in phases without undue further delay[9].
データ侵害はそれ自体が問題であるが、データの安全体制が脆弱、あるいは古くなっている兆候でもありえ、つまり侵害がシステム上に対応が必要な弱点があることを示している場合もありうる。一般的な事実として、データ侵害による被害にはその性質上不可逆的なものもあるため、事前準備によってデータ侵害を防止することが常により望ましい。管理者は、何らかの形式の攻撃に起因する侵害から発生するリスクを*詳細に*評価する前に、そのインシデントを引き起こした脆弱性がまだ存在するかどうか、それが依然悪用可能かどうかを見極めるために、問題の根本的原因を特定しなければならない。多くの場合、管理者は、そのインシデントがリスクを発生させるおそれがあり、従って通知を要すると特定することができる。それ以外の場合、侵害に関わるリスク及び影響が完全に評価されるまで通知を延期する必要はない。完全なリスク評価は通知と並行して行うことが可能であり、またその際に得られた情報は、更なる不当な遅滞なく、その状況に応じて SA に提供することができる[9]からである。

9. The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.
管理者は、その侵害がデータ主体の権利及び自由に対するリスクを発生させるおそれがあるという意見を持つ場合、これを通知しなければならず、侵害に気づいた時点でこの評価を行わなければならない。管理者は、詳細なフォレンジック調査及び（早期の）低減の手だてを待たずに、データ侵害がリスクを発生させるおそれがあるか、そのために通知する必要があるかを評価しなければならない。

10. If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the competent SA can use its corrective powers and may resolve to sanctions
リスクを発生させるおそれがないと管理者自身が評価したにもかかわらず、そのリスクが生じる場合、所轄 SA は是正権限を行使することができ、また制裁を科しうる。

[8] GDPR Article 34(1). GDPR 第 34 条第 1 項
[9] GDPR Article 33(4). GDPR 第 33 条第 4 項

11. Every controller and processor should have plans, procedures in place for handling eventual data breaches. Organisations should have clear reporting lines and persons responsible for certain aspects of the recovery process
全ての管理者及び処理者は、結果として起こるデータ侵害に対応するための計画を保持しておく、つまり手順を確立しておかなければならない。組織は、明確な報告ライン及び復元プロセスの特定部分の責任者を決めておかなければならない。

12. Training and awareness on data protection issues for the staff of the controller and processor focusing on personal data breach management (identification of a personal data breach incident and further actions to be taken, etc.) is also essential for the controllers and processors. This training should be regularly repeated, depending on the type of the processing activity and size of the controller, addressing latest trends and alerts coming from cyberattacks or other security incidents.
管理者及び処理者にとって、その職員を対象とした、個人データ侵害の管理（個人データ侵害インシデントの特定及びその次に取るべき行動等）に焦点をあてた、データ保護の問題についての訓練及び意識向上も必要不可欠である。この訓練は、取扱活動の種類及び管理者の規模に応じて、またサイバーアタック又はその他の安全上のインシデントの最新の傾向及び警告に対応しつつ、定期的に実施しなければならない。

13. The principle of accountability and the concept of data protection by design could incorporate analysis that feeds into a data controller's and data processor's own "Handbook on Handling Personal Data Breach" that aims to establish facts for each facet of the processing at each major stage of the operation. Such a handbook prepared in advance would provide a much quicker source of information to allow data controllers and data processors to mitigate the risks and meet the obligations without undue delay. This would ensure that if a personal data breach was to occur, people in the organisation would know what to do, and the incident would more than likely be handled quicker than if there were no mitigations or plan in place.
データ管理者及びデータ処理者自身の「個人データ侵害対応に関するハンドブック」に入る分析は、アカウンタビリティの原則及びデータ保護バイデザインの概念により盛込まれるかもしれない。当該ハンドブックは、業務の主要段階ごとの各取扱いについて立証することを目的とするものである。事前に準備されたこのようなハンドブックは、データ管理者及びデータ処理者がリスクを低減し、不当に遅滞なく義務を果たすことを可能にするための情報源をより迅速に提供するであろう。これにより、データ侵害が発生した際、組織内の人間は何をするべきかを認識し、低減措置又は計画がない場合に比べより迅速に当該侵害に対応することが確保されるであろう。

14. Though the cases presented below are fictitious, they are based on typical cases from the SA's collective experience with data breach notifications. The analyses offered relate explicitly to the cases under scrutiny, but with the goal to provide assistance for data controllers in assessing their own data breaches. Any modification in the circumstances of the cases described below may result in different or more significant levels of risk, thus requiring different or additional measures. These guidelines structure the cases according to certain categories of breaches (e.g. ransomware attacks). Certain mitigating measures are called for in each case when dealing with a certain category of breaches. These measures are not necessarily repeated in each case analysis belonging to the same category of breaches. For the cases belonging to the same category only the differences are laid out. Therefore, the reader should read all cases relevant to relevant category of a

breach to identify and distinguish all the correct measures to be taken.
次に述べる事例は架空のものであるが、データ侵害通知に関する SA の経験の集約からの典型的なケースに基づいたものである。提供された分析は、明示的に精査下のケースに関連しているが、データ管理者がデータ侵害を評価する際の支援を提供することを目的としている。下記の事例について、状況に何らかの変更が生じる場合には、異なるリスク又はより重大なレベルのリスクが生じうるため、異なる措置又は追加的な措置が必要となりうる。本ガイドラインは、一定の種類の侵害（ランサムウェア攻撃等）に応じて事例を構成している。ある種類の侵害に対応する場合、当該種類の侵害の各事例において、一定の低減措置が必要となる。こういった措置は、同一の種類の侵害に属する各事例の分析において必ずしも繰り返し記載されていない。同一の種類の侵害に属する事例については、措置の違いのみ記載されている。従って、全ての適正な措置を特定し識別するためには、該当の種類の侵害に関する全ての事例を読まなければならない。

15. The internal documentation of a breach is an obligation independent of the risks pertaining to the breach, and must be performed in each and every case. The cases presented below try to shed some light on whether or not to notify the breach to the SA and communicate it to the data subjects affected.
侵害の内部文書化は、侵害に関連するリスクに関わらず必要な義務であり、どのケースにおいても実施しなければならない。次に掲げる事例は、SA に対する侵害の通知及び影響を受けたデータ主体に対する侵害の連絡をするか否かについて明らかにすることを試みるものである。

2 RANSOMWARE
2 ランサムウェア攻撃

16. A frequent cause for a data breach notification is a ransomware attack suffered by the data controller. In these cases a malicious code encrypts the personal data, and subsequently the attacker asks the controller for a ransom in exchange for the decryption code. This kind of attack can usually be classified as a breach of availability, but often also a breach of confidentiality could occur.
データ侵害通知の原因の多くは、データ管理者が被るランサムウェア攻撃である。これらの場合、個人データが悪意のあるコードにより暗号化され、その後攻撃者が管理者に対し、その復号コードと引き換えに身代金を要求する。この種の攻撃は、通常可用性の侵害として分類されうるが、しばしば機密性の侵害として分類される場合もある。

2.1 CASE No. 01: Ransomware with proper backup and without exfiltration
2.1 事例 No.01：ランサムウェア攻撃（適正なバックアップ有、データ流出無）

Computer systems of a small manufacturing company were exposed to a ransomware attack, and data stored in those systems was encrypted. The data controller used encryption at rest, so all data accessed by the ransomware was stored in encrypted form using a state-of-the-art encryption algorithm. The decryption key was not compromised in the attack, i.e. the attacker could neither access it nor use it indirectly. In consequence, the attacker only had access to encrypted personal data. In particular, neither the email system of the company, nor any client systems used to access it were affected. The company is using the expertise of an external cybersecurity company to investigate the incident. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data collected by the

detection systems the company has deployed, an internal investigation supported by the external cybersecurity company determined *with certainty* that the perpetrator only encrypted data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to clients and employees of the company, a few dozen individuals altogether. A backup was readily available, and the data was restored a few hours after the attack took place. The breach did not result in any consequences on the day-to-day operation of the controller. There was no delay in employee payments or handling client requests.
ある小規模製造会社のコンピュータシステムがランサムウェア攻撃にさらされ、システムに記録保存されていたデータが暗号化された。データ管理者は保存時の暗号化を使用していたため、ランサムウェアにアクセスされた全てのデータは最新の暗号化アルゴリズムにより暗号化された形式で保存されていた。当該復号鍵は攻撃による侵害を受けなかった。つまり、攻撃者がデータへアクセスする可能性も間接的に使用する可能性もない。結果、攻撃者は暗号化された個人データにアクセスしたのみであった。特に、同社の電子メールシステムも、これにアクセスするために用いる顧客システムも影響を受けなかった。同社は外部のサイバーセキュリティ企業の専門知識を活用してインシデント調査を行っている。同社からの全てのデータの流れ（外部に送信される電子メールを含む）を追跡したログが利用可能である。当該ログ及び同社が導入している侵害検知システムが収集したデータの分析の結果、外部のサイバーセキュリティ企業のサポートを受けて実施された内部調査は、犯人はデータを暗号化しただけであり、データの窃取はなかったと*確信*をもって判断した。当該ログは、攻撃の間、外部へのデータの流れが無いことを示している。侵害により影響を受けた個人データは、同社の顧客及び従業員、計数十名に関わるものである。バックアップが即座に使用でき、データは攻撃後数時間で復元された。当該侵害により管理者の日常業務への影響は生じなかった。従業員への支払い又は顧客の要望への対応に遅延はなかった。

17. In this case, the following elements were realized from the definition of a 'personal data breach': a breach of security led to unlawful alteration and unauthorized access to personal data stored.
この事例では、「個人データ侵害」の定義のうち次の要素が生じた。違法な改変及び無権限のアクセスを導くような記録保存された個人データの安全性に対する侵害。

2.1.1 CASE No. 01 - Prior measures and risk assessment
2.1.1 事例 No.01—事前対策及びリスク評価

18. As with all risks posed by external actors, the likelihood that a ransomware attack is successful can be drastically reduced by tightening the security of the data controlling environment. The majority of these breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. Examples of such measures are proper patch management and the use of an appropriate anti-malware detection system. Having a proper and separate backup will help to mitigate the consequences of a successful attack should it occur. Moreover, an employee security education, training, and awareness (SETA) program, will help to prevent and recognise this kind of attack. (A list of advisable measures can be found in section 2.5.) Among those measures, a proper patch management that ensures that the systems are up to date and all known vulnerabilities of the deployed systems are fixed is one of the most important since most of the ransomware attacks exploit well known vulnerabilities.
外部の行為主体によってもたらされる全てのリスクの場合と同様、データ管理環

境の安全性の強化により、ランサムウェア攻撃が成功する蓋然性を劇的に下げることができる。このような侵害の多くは、適切な組織的、物理的及び技術的な安全管理措置の確保により防止することができる。そのような措置の例として、適正なパッチ管理及び適切なマルウェア検知システムの使用がある。適正かつ独立したバックアップを保持することは、万一攻撃が成功した場合、その攻撃の影響を低減することに役立つ。さらに、従業員のセキュリティ教育、訓練及び認識（SETA）プログラムもこうした攻撃の防止及び認識に役立つ。（望ましい措置のリストは本ガイドライン第 2.5 節を参照。）とりわけ、ランサムウェア攻撃の大半は広く認知されている脆弱性を利用しているため、適正なパッチ管理によりシステムを最新状態に維持し、導入されているシステムの全ての既知の脆弱性を修正するよう確保することが、最も重要な措置の一つである。

19. When assessing the risks, the controller should investigate the breach and identify the type of the malicious code to understand the possible consequences of the attack. Among those risks to be considered is the risk that data was exfiltrated without leaving a trace in the logs of the systems.
リスク評価を行う際、管理者は、攻撃により生じうる影響について理解するため、侵害を調査し、悪意のあるコードの種類を特定しなければならない。これらのリスクの中で考えられるリスクとして、システムログに痕跡を残さずにデータが窃取されているリスクがある。

20. In this example, the attacker had access to personal data and the confidentiality of cipher text containing personal data in encrypted form was compromised. However, any data that might have been exfiltrated cannot be read or used by the perpetrator, at least for the time being. The encryption technique used by the data controller conforms to the state-of-the-art. The decryption key was not compromised and presumably could also not be determined by other means. In consequence, the confidentiality risks to the rights and freedoms of natural persons are reduced to a minimum barring cryptanalytic progress that renders the encrypted data intelligible in the future.
この事例では、攻撃者が個人データにアクセスし、暗号化された形式での個人データを含む暗号文の機密性が侵害された。しかし、少なくとも当面の間、窃取された可能性のあるいかなるデータも、犯人に読まれたり使用されたりする可能性はない。データ管理者は最新技術に適合した暗号化技術を使用している。当該復号鍵は侵害されておらず、また恐らく他の手段により当該複合鍵を判明することもできていないであろう。結果、自然人の権利及び自由に対する機密性のリスクは、将来暗号解読技術の進歩により暗号化されたデータの解読が可能にならない限り、最小限に抑えられる。

21. The data controller should consider the risk to individuals due to the breach[10]. In this case, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not

[10] For guidance on "likely to result in high risk" processing operations, see A29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", WP248 rev. 01, - endorsed by EDPB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、第 29 条作業部会、「データ保護影響評価（DPIA）及び取扱いが規則 2016/679 の適用上「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン」、WP 248 rev. 01、EDPB 承認版、https://ec.europa.eu/newsroom/article29/items/611236 、P9 を参照のこと。

compromised[11]. In this example, the adverse effects of the breach were mitigated fairly soon after the breach occurred. Having a proper backup regime[12] makes the effects of the breach less severe and here the controller was able to effectively make use of it.
データ管理者は侵害が個人にもたらすリスクについて考えなければならない [10]。この事例の場合、データ主体の権利及び自由に対しもたらされるリスクは個人データの可用性の欠落から生ずるものであり、機密性は侵害されていないと考えられる [11]。この例では、当該侵害による悪影響は、侵害発生後短時間で低減された。適正なバックアップ体制 [12] を保持することは、侵害による影響の深刻度を低減させる。そしてここでは、管理者は適正なバックアップ体制を効果的に利用することができている。

22. On the severity of the consequences for the data subjects, only minor consequences could be identified since the affected data was restored in a few hours, the breach did not result in any consequences on the day-to-day operation of the controller and had no significant effect on the data subjects (e.g. employee payments or handling client requests).
データ主体に対する影響の深刻度については、影響を受けたデータが数時間で復元され、結果として、侵害により管理者の日常業務に影響はなく、またデータ主体に対する（例えば、従業員に対する支払又は顧客の要望への対応への）重大な影響もなかったことから、小さい影響のみ確認されるであろう。

2.1.2 CASE No. 01 – Mitigation and obligations
2.1.2 事例 No.01—リスク低減措置及び義務

23. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again. In this particular case however, the impacts of the attack could effectively be contained by resetting all compromised systems to a clean state known to be free of malicious code, fixing the vulnerabilities and restoring the affected data soon after the attack. Without a backup, data is lost and the severity may increase because risks or impacts to individuals may also do so.

[11] Technically, encryption of data will involve “access” to original data, and in the case of ransomware, the deletion of the original – the data needs to be accessed by ransomware code to encrypt it, and to remove the original data. An attacker may take a copy of the original before deletion, but personal data will not always be extracted. As a data controller’s investigation progresses, new information may come to light to make this assessment change. Access that results in unlawful destruction, loss, alteration, unauthorised disclosure of the personal data, or to a security risk to a data subject, even without interpretation of the data may be as severe as access with interpretation of the personal data.
技術上、データの暗号化はオリジナルデータへの「アクセス」に関わることであり、ランサムウェアの場合はこれにオリジナルデータの消去が加わる。つまりデータを暗号化するためにはランサムウェアコードがデータにアクセスし、かつ当該オリジナルデータを消去する必要がある。攻撃者はオリジナルデータを消去する前に当該オリジナルデータの複製を取得しうるが、個人データが必ずしも窃取されるとは限らない。データ管理者の調査が進むにつれ、新たな情報が判明し、評価が変わる場合がある。個人データの違法な破壊、喪失、改変、無権限の開示、又はデータ主体に対する安全性のリスクを発生させるアクセスは、データの解読がされない場合であっても、個人データが解読される場合と同様に深刻でありうる。

[12] Backup procedures should be structured, consistent and repeatable. Examples of back up procedures are the 3-2-1 method and the grandfather-father-son method. Any method should always be tested for effectiveness in coverage and when data is to be restored. Testing should also be repeated at intervals and especially when changes occur in the processing operation or its circumstances to ensure the integrity of the system.
バックアップの手順は、構造化され、一貫性があり、反復可能でなければならない。バックアップの手順の例として、3-2-1 ルールの方式及び 3 世代管理の方式がある。いずれの方法においても対象範囲の有効性及びいつデータが復元されるかについて常にテストしておかなければならない。テストはまた、間隔を置いて繰り返し、特にシステムの完全性を確保するため、取扱業務又はその状況に変更があった場合に実施されなければならない。

バックアップがない場合、失われた個人データを復元するために管理者が実施できる措置はほとんどなく、データは再度収集されなければならない。しかしこの特定の事例では、侵害を受けた全てのシステムを悪意のあるコードがない状態であるクリーンな状態にリセットし、脆弱性を修正し、影響を受けたデータを攻撃後すぐに復元することにより、攻撃の影響を効果的に抑えることができた。バックアップがない場合、データは喪失し、個人に対するリスク又は影響も大きくなりうることから、深刻度も上昇しうる。

24. The timeliness of an effective data restoration from the readily available backup is a key variable when analysing the breach. Specifying an appropriate timeframe to restore the compromised data depends on the unique circumstances of the breach at hand. The GDPR states that a personal data breach shall be notified without undue delay and, where feasible, not later than after 72 hours. Therefore, it could be determined that exceeding the 72-hour time limit is unadvisable in any case, but when dealing with high risk level cases, even complying with this deadline can be viewed as unsatisfactory.
容易に利用可能なバックアップから効果的にデータ復元を行うといった適時性は、侵害の分析において主要な変動要因となる。不正なアクセスを受けたデータを復元するための適切なタイムフレームは、該当する侵害の固有の状況に応じて特定される。GDPR は、個人データ侵害は、不当な遅滞なく、かつ、それが実施可能なときは、72 時間以内に通知することとしている。そのため、いかなる場合でも 72 時間の時間制限を超えることは望ましくないと判断されるかもしれないが、高いリスクレベルのケースを取扱う場合においては、72 時間の時間制限を遵守したとしても不十分とみなされる可能性がある。

25. In this case, following a detailed impact assessment and incident response process, the controller determined that the breach was unlikely to result in a risk to the rights and freedoms of natural persons, hence no communication to the data subjects is necessary, nor does the breach require a notification to the SA. However, as all data breaches, it should be documented in accordance with Article 33 (5). The organisation may also need (or later be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures. Within the frame of this update and remediation, the organisation should thoroughly investigate the breach and identify the causes and the methods used by the perpetrator in order to prevent any similar events in the future.
この事例では、管理者は、詳細な影響評価及びインシデント対応プロセスの実施の結果、当該侵害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はなく、よってデータ主体に対する連絡及び SA に対する通知は必要ないと判断した。しかし、全てのデータ侵害同様、GDPR 第 33 条第 5 項に基づき侵害について文書化しなければならない。また同社において、その組織的及び技術的な個人データの安全な取扱い並びにリスク低減措置及び手順の更新並びに改善が必要となりうる（又は後に SA から要請されうる）。同社は、当該更新及び改善を実施するなかで、今後同様の事態の発生を防止するために、当該侵害を徹底的に調査し、侵害の原因及び犯人が使用した方法を特定しなければならない。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

2.2 CASE No. 02: Ransomware without proper backup
2.2 事例 No.02：ランサムウェア攻撃（適正なバックアップ無）

One of the computers used by an agricultural company was exposed to a ransomware attack and its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data, without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and clients of the company, a few dozen individuals altogether. No special categories of data were affected. No backup was available in an electronic form. Most of the data was restored from paper backups. The restoration of the data took 5 working days and led to minor delays in the delivery of orders to customers.

ある農業関係の会社が使用するコンピュータの 1 つがランサムウェア攻撃にさらされ、そのデータが攻撃者により暗号化された。同社は外部のサイバーセキュリティ企業の専門知識を活用してネットワークを監視している。同社からの全てのデータの流れ（外部に送信される電子メールを含む）を追跡したログが利用可能である。当該ログ及び他の検知システムが収集したデータの分析の結果、サイバーセキュリティ企業のサポートを受けて実施された内部調査は、犯人はデータを暗号化しただけであり、データの窃取はなかったと判断した。当該ログは、攻撃の間、外部へのデータの流れが無いことを示している。侵害により影響を受けた個人データは、同社の従業員及び顧客、計数十名に関わるものである。特別な種類のデータは影響を受けていない。電子的な形式でのバックアップは無かった。大部分のデータは紙媒体のバックアップから復元された。データの復元に 5 営業日を要し、顧客への注文の納品に軽微な遅延が生じた。

2.2.1 CASE No. 02 - Prior measures and risk assessment
2.2.1 事例 No.02—事前対策及びリスク評価

26. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.9※. The major difference to the previous case is the lack of an electronic backup and the lack of encryption at rest. This leads to critical differences in the following steps.

データ管理者は、本ガイドライン第 2.1 節及び第 2.9 節※に記載のものと同様の事前の対策を適用しておくべきであった。前の事例との主な違いは、電子的なバックアップの欠如及びデータ保存時の暗号化の欠如である。これにより、続く手だてに決定的な違いが生じてくる。

※仮訳者注：望ましい措置のリストは、第 2.5 節に説明がある。当該ガイドライン内には第 2.9 節は存在せず、ここではパラグラフ 18 同様、第 2.5 節を言及しているものと考えられる。

27. When assessing the risks, the controller should investigate the method of infiltration and identify the type of the malicious code to understand the possible consequences of the attack. In this example the ransomware encrypted the personal data without exfiltrating it. As a result, it appears the risks to the rights and freedoms of data subjects result from the lack of availability of the personal data, and the confidentiality of the personal data is not compromised. A thorough examination of the firewall logs and its implications is essential

in determining the risk. The data controller should present the factual findings of these investigations upon request.
リスク評価を行う際、管理者は、攻撃により生じうる影響について理解するため、侵入方法を調査し、悪意のあるコードの種類を特定しなければならない。この事例では、ランサムウェアにより個人データが暗号化されたが、窃取はされなかった。その結果、データ主体の権利及び自由に対しもらたされたリスクは個人データの可用性が失われたことから生じるものであり、個人データの機密性への侵害はないと想定される。リスクを判断する際、ファイアウォールのログ及びそこから導かれる事項の徹底的な調査が必須である。データ管理者は要請に応じてこれらの調査から明らかになった事実を提示しなければならない。

28. The data controller needs to keep in mind that if the attack is more sophisticated the malware has the functionality to edit log files and remove the trace. So - given that logs are not forwarded or replicated to a central log server - even after a thorough investigation that determined that the personal data was not exfiltrated by the attacker, the data controller cannot state that the absence of a log entry proves the absence of exfiltration, therefore the likelihood of a confidentiality breach cannot be entirely dismissed.
データ管理者は、より高度化した攻撃の場合、ログファイルを編集し痕跡を削除する機能がマルウェアにはあることを念頭に置かなければならない。従って、もし中央管理のログサーバーへのログの転送又は複製を行っていない場合、徹底的な調査により個人データが攻撃者により窃取されていないと判断された後であっても、データ管理者はログエントリがないことがデータの流出がないことを証明しているとは断言できないため、機密性の侵害の蓋然性を完全に否定することはできない。

29. The data controller should assess the risks of this breach[13] if the data was accessed by the attacker. During the risk assessment, the data controller should also take into consideration the nature, the sensitivity, the volume, and the context of personal data affected in the breach. In this case no special categories of personal data are affected, and the quantity of breached data and the number of affected data subjects is low.
データが攻撃者によりアクセスされた場合、データ管理者は当該侵害のリスクを評価しなければならない。リスク評価の中でデータ管理者はまた、当該侵害により影響を受けた個人データの性質、機微性、量及び過程を考慮に入れなければならない [13]。この事例では特別な種類の個人データは影響を受けておらず、侵害を受けたデータの量及び影響を受けたデータ主体の数は少ない。

30. Gathering exact information on the unauthorized access is key for determining the risk level and preventing a new or continued attack. If the data had been copied from the database, it would obviously have been a risk-increasing factor. When uncertain about the specifics of the illegitimate access, the worse scenario should be considered and the risk should be assessed accordingly.
リスクレベルを決定し、また新たな又は継続的な攻撃を防止するために、当該無権限のアクセスについて正確な情報を収集することが重要である。データがデータベースから複製されていた場合、このことは明らかにリスクを高める要素となっていたであろう。違法アクセスの詳細が確かではない場合、より悪いシナリオを考慮し、それに基づきリスクを評価しなければならない。

31. The absence of a backup database can be considered a risk enhancing factor depending on

[13] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.
*「高いリスクをもたらすおそれのある」*取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

the severity of consequences for the data subjects resulting from the lack of availability of the data.
データベースのバックアップが存在しないことは、データの可用性の欠如から生じるデータ主体に及ぼす影響の深刻度に応じて、リスクを高める要素とみなされる可能性がある。

2.2.2 CASE No. 02 – Mitigation and obligations
2.2.2 事例 No.02—リスク低減措置及び義務

32. Without a backup few measures to remediate the loss of personal data can be undertaken by the controller, and the data has to be collected again, unless some other source is available (e.g. order confirmation e-mails). Without a backup, data may be lost and the severity will depend on the impact for the individuals.
バックアップがない場合、失われた個人データを復元するために管理者が実施できる措置はほとんどなく、他の情報源（注文確認の電子メール等）が利用可能な場合を除き、データは再度収集されなければならない。バックアップがない場合、データは失われるおそれがあり、その深刻度は個人に及ぼす影響により異なる。

33. The restoration of the data should not prove to be overly problematic[14] if the data is still available on paper, but given the lack of an electronic backup database, a notification to the SA is considered necessary, as the restoration of the data took some time and could cause some delays in the orders' delivery to customers and a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.
データがそれでも紙媒体で利用可能な場合、データの復元が過度に問題となることはないであろうが [14]、電子的なバックアップのデータベースが無いならば、データの復元に時間を要し、顧客への注文の納品に遅れが生じる可能性があり、また相当量のメタデータ（ログ、タイムスタンプ等）が回収できないおそれがあるため、SA に対する通知が必要とみなされる。

34. Informing the data subjects about the breach may also depend on the length of time the personal data is unavailable and the difficulties it might cause in the operation of the controller as a result (e.g. delays in transferring employee's payments). As these delays in payments and deliveries may lead to financial loss for the individuals whose data has been compromised, one could also argue the breach is likely to result in a high risk. Also, it might not be possible to avoid informing the data subjects if their contribution is needed for restoring the encrypted data.
データ主体に対する侵害通知についても、個人データを使用できない時間の長さ、及びそれが結果的に管理者の業務にもたらすかもしれない困難度（従業員に対する送金の遅延等）によって異なりうる。支払及び納品の遅延により、そのデータが侵害された個人にとって金銭上の損失につながりうるため、侵害が高いリスクを発生させるおそれがあると主張される可能性もある。また、暗号化されたデータの復元にデータ主体からの情報の提供が必要となる場合は、データ主体に対する通知は避けられないであろう。

35. This case serves as an example for a ransomware attack with risk to the rights and

[14] This will depend on the complexity and structure of the personal data. In the most complex scenarios, re-establishing data integrity, consistency with metadata, ensuring the correct relationships within data structures and checking data accuracy may take significant resources and effort.
これは個人データの複雑さ及び構造により異なる。最も複雑な場合では、データの完全性、つまりメタデータとの整合性の復元、データ構造内の適正な関係性の確保及びデータの正確性の確認のために、多大なリソース及び労力が必要となりうる。

freedoms of the data subjects, but not reaching high risk. It should be documented in accordance with Article 33 (5) and notified to the SA in accordance with Article 33 (1). The organisation may also need (or be required by the SA) to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
この事例は、データ主体の権利及び自由に対するリスクがあるが、高いリスクには至らないランサムウェア攻撃の一例である。第 33 条第 5 項に基づく文書化、及び第 33 条第 1 項に基づく SA に対する通知を行わなければならない。同社はまた、その組織的及び技術的な個人データの安全な取扱い並びにリスク低減措置及び手順の更新並びに改善が必要となりうる（又は SA から要請されうる）。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	X

2.3 CASE No. 03: Ransomware with backup and without exfiltration in a hospital
2.3 事例 No.03：病院におけるランサムウェア攻撃（バックアップ有、データ流出無）

The information system of a hospital / healthcare centre was exposed to a ransomware attack and a significant proportion of its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and patients, which represented thousands of individuals. Backups were available in an electronic form. Most of the data was restored but this operation lasted 2 working days and led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering the level of service due to the unavailability of the systems.
ある病院／医療施設の情報システムがランサムウェア攻撃にさらされ、攻撃者によりデータの大部分が暗号化された。同院は外部のサイバーセキュリティ企業の専門知識を活用してネットワークを監視している。同院からの全てのデータの流れ（外部に送信される電子メールを含む）を追跡したログが利用可能である。当該ログ及び他の検知システムが収集したデータの分析の結果、外部のサイバーセキュリティ企業のサポートを受け実施した内部調査は、犯人はデータを暗号化しただけであり、データの窃取はなかったと判断した。当該ログは、攻撃の間、外部へのデータの流れが無いことを示している。侵害により影響を受けた個人データは、従業員及び患者、数千人に関わるものである。電子的な形式でのバックアップは利用可能であった。ほとんどのデータは復元されたが、その作業は 2 営業日続き、手術の中止又は延期を伴う患者の治療への大幅な遅延やシステムの使用不能による医療提供水準の低下につながった。

2.3.1 CASE No. 03 - Prior measures and risk assessment
2.3.1 事例 No.03—事前対策及びリスク評価

36. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. The major difference to the previous case is the high severity of consequences for a substantial part of the data subjects[15].
データ管理者は、本ガイドライン第 2.1 節及び第 2.5 節に記載のものと同様の事前の対策を適用しておくべきであった。前の事例との主な違いは、データ主体の大部分に深刻度の高い影響をもたらしたことである [15]。

37. The quantity of breached data and the number of affected data subjects are high, because hospitals usually process large quantities of data. The unavailability of the data has a high impact on a substantial part of the data subjects. Moreover, there is a residual risk of high severity to the confidentiality of the patient data.
病院は通常、大量のデータを取扱っているため、侵害を受けたデータの量及び影響を受けたデータ主体の数は多い。データの使用不能は、データ主体の大部分に大きな影響をもたらす。さらに、患者のデータの機密性に対する深刻度の高い残存リスクがある。

38. The type of the breach, nature, sensitivity, and volume of personal data affected in the breach are important. Even though a backup for the data existed and it could be restored in a few days, a high risk still exists due to the severity of consequences for the data subjects resulting from the lack of availability of the data at the moment of the attack and the following days.
侵害の種類、侵害の影響を受けた個人データの性質、機微性及び量は重要である。データのバックアップが存在し数日でデータを復元できるとしても、攻撃の時点及びその後の数日間にわたるデータの使用不能から生じるデータ主体への影響の深刻度から、高いリスクが依然存在する。

2.3.2 CASE No. 03 – Mitigation and obligations
2.3.2 事例 No.03—リスク低減措置及び義務

39. A notification to the SA is considered necessary, as special categories of personal data are involved and the restoration of the data could take a long time, resulting in major delays in patient care. Informing the data subjects about the breach is necessary due to the impact for the patients, even after restoring the encrypted data. While data relating to all patients treated in the hospital during the last years have been encrypted, only those patients who were scheduled to be treated in the hospital during the time the computer system was unavailable were impacted. The controller should communicate the data breach to those patients directly. Direct communication to the other patients some of which may not have been in the hospital for more than twenty years may not be required due to the exception in Article 34 (3) c). In such a case, there shall instead be a public communication[16] or similar

[15] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

[16] GDPR Recital 86 explains that "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".
GDPR の前文第 86 項では「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

measure whereby the data subjects are informed in an equally effective manner. In this case, the hospital should make the ransomware attack and its effects public.
特別な種類の個人データが関係していること、またデータの復元に時間を要し、その結果患者の治療に大幅な遅延が生じる可能性があることから、SA への通知は必要とみなされる。暗号化されたデータの復元後も、患者に及ぼす影響から、データ主体に対する侵害の連絡は必要である。過去複数年間に同院で治療を受けた全ての患者に関わるデータが暗号化されたが、影響を受けたのはコンピュータシステムの使用不能期間中に同院で治療を受ける予定であった患者のみである。管理者は、当該患者に対し、データ侵害について直接連絡しなければならない。20 年以上来院していなかった可能性のある患者を含むその他の患者に対する直接の連絡は、第 34 条第 3 項(c)の例外に基づき要求されない。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 [16]。この事例の場合、同病院はランサムウェア攻撃及びその影響について公表しなければならない。

40. This case serves as an example for a ransomware attack with high risk to the rights and freedoms of the data subjects. It should be documented in accordance with Article 33 (5), notified to the SA in accordance with Article 33 (1) and communicated to the data subjects in accordance with Article 34 (1). The organisation also needs to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
この事例は、データ主体の権利及び自由に対する高いリスクがあるランサムウェア攻撃の一例である。第 33 条第 5 項に基づく文書化、第 33 条第 1 項に基づく SA に対する通知、及び第 34 条第 1 項に基づくデータ主体に対する連絡を行わなければならない。同病院はまた、その組織的及び技術的な個人データの安全な取扱い並びにリスク低減措置及び手順の更新並びに改善が必要となる。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

2.4 CASE No. 04: Ransomware without backup and with exfiltration
2.4 事例 No.04：ランサムウェア攻撃（バックアップ無、データ流出有）

The server of a public transportation company was exposed to a ransomware attack and its data was encrypted by the attacker. According to the findings of the internal investigation the perpetrator not only encrypted the data, but also exfiltrated it. The type of breached data was the personal data of clients and employees, and of the several thousand people using the services of the company (e.g. buying tickets online). Beyond basic identity data, identity card numbers and financial data such as credit card details are involved in the breach. A backup database existed, but it was also encrypted

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。」と説明している。

by the attacker.
ある公共交通会社のサーバーがランサムウェア攻撃にさらされ、同社のデータが当該攻撃者により暗号化された。内部調査の結果によると、犯人はデータを暗号化しただけでなく、窃取もしていた。侵害されたデータの種類は、顧客及び従業員の個人データ、並びに同社のサービス（オンラインでのチケット購入、等）の利用者数千人の個人データである。基本的な身元データだけでなく、身分証明書の番号及びクレジットカード情報といった財務データも当該侵害に関与している。バックアップデータは存在するが、これも攻撃者により暗号化された。

2.4.1 CASE No. 04 - Prior measures and risk assessment
2.4.1 事例 No.04—事前対策及びリスク評価

41. The data controller should have adopted the same prior measures as mentioned in part 2.1. and in section 2.5. Though backup was in place, it was also affected by the attack. This arrangement alone raises questions about the quality of the controller's prior IT security measures and should be further scrutinised during the investigation, since in a well-designed backup regime, multiple backups must be securely stored without access from the main system, otherwise they could be compromised in the same attack. Furthermore, ransomware attacks may lie undiscovered for days slowly encrypting rarely used data. This can render multiple backups useless, so backups should also be taken periodically and be isolated. This would increase the likelihood of recovery albeit with increased loss data.
データ管理者は、本ガイドライン第 2.1 節及び第 2.5 節に記載のものと同様の事前の対策を適用しておくべきであった。バックアップデータはあったが、これも攻撃の影響を受けた。このことは、それだけで管理者の事前の IT の安全管理措置の質について疑問を提示し、調査を実施する中で更に詳細に調べられなければならない。何故なら適切に設置されたバックアップ体制の下では、複数のバックアップを主システムに接続することなく安全に保存することが求められる。さもなくば、同一の攻撃で複数のバックアップが侵害を受ける可能性があるからである。更に、ランサムウェア攻撃は、使用頻度の低いデータを徐々に暗号化しつつ、数日間発見されないまま存在する場合がある。これにより複数のバックアップが使用不能となる可能性があるため、バックアップを定期的に作成し、切り離しておかなければならない。これによりデータの喪失の増大にかかわらず復元の蓋然性は高まるであろう。

42. This breach concerns not only data availability, but confidentiality as well, since the attacker may have modified and / or copied data from the server. Therefore, the type of the breach results in high risk[17].
攻撃者がサーバーからデータを改変及び／又は複製しているおそれがあるため、当該侵害はデータの可用性だけでなく機密性にも関わる。そのため、この種類の侵害は高いリスクをもたらす[17]。

43. The nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data. Beyond basic identity data, identity documents and financial data such as credit card details are involved too. A data breach concerning these types of data presents high risk in and of themselves, and if processed together, they could be used for – among others - identity theft or fraud.

[17] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

影響を受けた個人データの総量同様、影響を受けた個人の数が多いため、個人データの性質、機微性及び量によってリスクはさらに高くなる。基本的な身元データだけでなく、身分証明書及びクレジットカード情報といった財務データも影響を受けている。これらの種類のデータに関する侵害は、それ自体でリスクが高く、もし一緒に取扱われると、特に、ID 盗取又は ID 詐欺に使用される可能性がある。

44. Due to either faulty server logic or organizational controls, the backup files were affected by the ransomware, preventing the restore of data and enhancing the risk.
サーバーのロジック又は組織の管理体制の欠陥のいずれかによりバックアップファイルがランサムウェア攻撃の影響を受け、これによりデータを復元することができず、リスクが高まった。

45. This data breach presents a high risk to the rights and freedoms of individuals, because it could likely lead to both material (e.g. financial loss since credit card details were affected) and non-material damage (e.g. identity theft or fraud since identity card details were affected).
当該データ侵害は、財産的な損失（クレジットカード情報が影響を受けたことによる金銭的損失、等）及び非財産的な損失（ID カード情報が影響を受けたことによる ID 盗取又は ID 詐欺、等）の両方に繋がる可能性があるため、個人の権利及び自由に対する高いリスクをもたらす。

2.4.2 CASE No. 04 – Mitigation and obligations
2.4.2 事例 No.04—リスク低減措置及び義務

46. Communication to the data subjects is essential, so they can make the necessary steps to avoid material damage (e.g. block their credit cards).
データ主体が財産的な損失を回避するための必要な手だて（クレジットカードの停止、等）を講じることができるよう、データ主体への連絡は必須である。

47. Aside from documenting the breach in accordance with Article 33 (5), a notification to the SA is also mandatory in this case (Article 33 (1)) and the controller is also obliged to communicate the breach to the data subjects (Article 34 (1)). The latter could be undertaken on a person-by-person basis, but for individuals where contact data is not available the controller should do so publicly, provided that such communication would not be susceptible to trigger additional negative consequences on the data subjects, e.g. by way of a notification on its website. In the latter case a precise and clear communication is required, in plain sight on the homepage of the controller, with exact references of the relevant GDPR provisions. The organisation may also need to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures.
この事例では、第 33 条第 5 項に基づく文書化のほか、SA に対する通知が必須であり（第 33 条第 1 項）、また管理者にはデータ主体に対する侵害の連絡の義務もある（第 34 条第 1 項）。データ主体に対する連絡は直接行うことができるが、連絡先データが使用できない個人については、当該連絡方法によりデータ主体に対し追加的な悪影響を引き起こすことにならない場合、管理者は、例えばウェブサイト上での通知といった方法で、公表による連絡をしなければならない。後者の場合には、管理者のホームページ上に視覚的に見やすい方法で、関連の GDPR 条項への的確な参照を含め、正確かつ明確な連絡をすることが要件となる。同社はまた、その組織的及び技術的な個人データの安全な取扱い並びにリスク低減措置及び手順の更新並びに改善が必要となりうる。

Actions necessary based on the identified risks 特定されたリスクに基づき必要となる措置		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

2.5 Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks

2.5 ランサムウェア攻撃の防止／影響低減のための組織的及び技術的な措置

48. The fact that a ransomware attack could have taken place is usually a sign of one or more vulnerabilities in the controller's system. This also applies in ransomware cases in which the personal data has been encrypted, but has not been exfiltrated. Regardless of the outcome and the consequences of the attack, the importance of an all-encompassing evaluation of the data security system - with particular emphasis on IT security - cannot be stressed enough. The identified weaknesses and security holes are to be documented and addressed without delay.
ランサムウェア攻撃が起こり得たという事実は通常、管理者のシステムに一つ以上の脆弱性があることを示している。このことは個人データが暗号化されたが窃取は無かったランサムウェア攻撃のケースにも当てはまる。攻撃の結果と影響にかかわらず、特に IT セキュリティに重点を置いた、データのセキュリティシステム全体の包括的な評価の重要性は、いくら強調してもし過ぎることはない。特定された弱点及びセキュリティホールについては文書化し、不当に遅滞なく対処しなければならない。

49. Advisable measures:
望ましい措置

(The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.)
（下記の措置のリストは、これ以外の措置を排除するものでも全てを網羅するものでもない。むしろ防止案及び考えられる解決策の提供を目的とするものである。取扱活動はそれぞれ異なるため、管理者は状況に応じて最適な措置を決定しなければならない。）

- Keeping the firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) up to date. Ensuring that appropriate IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. This includes keeping detailed logs of which patches are applied at which timestamp.
同一 LAN（Wi-Fi 装置を含む）上にあるサーバー、クライアントマシン、稼働中のネットワークコンポーネント及びその他の機械装置上のファームウェア、オペレーティングシステム及びアプリケーションソフトウェアを最新の状態に保つ。適切な IT の安全管理措置を設けることを確保し、それらを確実に有効な状態にし、取扱い若しくは状況に変更又は展開がある際は常に更新するよう維持する。これには、どのタイムスタンプにどのパッチが適用されているかの詳細

なログの維持も含まれる。

- Designing and organising processing systems and infrastructure to segment or isolate data systems and networks to avoid propagation of malware within the organisation and to external systems.
  組織内及び外部システムへのマルウェアの拡大を防止するため、データ管理システムとネットワークを区分する又は分離するよう処理システム及びインフラを設計及び構築する。
- The existence of an up-to-date, secure and tested backup procedure. Media for medium- and long-term back-up should be kept separate from operational data storage and out of reach of third parties even in case of a successful attack (such as daily incremental backup and weekly full backup).
  最新で、安全かつテスト済のバックアップ手順の存在。中長期的バックアップ（日次増分バックアップ及び週次フルバックアップなど）のための記憶媒体は、運用中のデータ・ストレージから切り離し、攻撃が成功した場合であっても第三者が接触できないように保管しておかなければならない。
- Having / obtaining an appropriate, up-to-date, effective and integrated anti-malware software.
  適切で、最新の、有効で、かつ統合されたマルウェア対策ソフトウェアを保持／入手する。
- Having an appropriate, up-to-date, effective and integrated firewall and intrusion detection and prevention system. Directing network traffic through the firewall/intrusion detection, even in the case of home office or mobile work (e.g. by using VPN connections to organizational security mechanisms when accessing the internet).
  適切で、最新の、有効で、かつ統合されたファイアウォール及び侵入検知・侵入防止システムを設置する。在宅勤務又はリモートワーク時においても、（例えば、インターネットアクセス時に組織的なセキュリティメカニズムへの VPN 接続を使用することにより）ファイアウォール／侵入検知システムを通してネットワークに接続させる。
- Training employees on the methods of recognising and preventing IT attacks. The controller should provide means to establish whether emails and messages obtained by other means of communication are authentic and trustworthy. Employees should be trained to recognize when such an attack has realized, how to take the endpoint out of the network and their obligation to immediately report it to the security officer.
  従業員に対し、IT 攻撃を認識し、また防止する方法に関する訓練を実施する。管理者は、異なる連絡手段で取得した電子メール及びメッセージの真正性と信頼性を確認する手段を提供すること。従業員は、このような攻撃がいつ起きていたか、どのように端末をネットワークから切離すか、また攻撃をセキュリティ責任者に直ちに報告する義務について認識すべく、訓練を受けなければならない。
- Emphasize the need of identifying the type of the malicious code to see the consequences of the attack and be able to find the right measures to mitigate the risk. In case a ransomware attack has succeeded and there is no back-up available, tools available such as the ones by the “no more ransom” (nomoreransom.org) project may be applied to retrieve data. However, in case a safe backup is available, restoring the data from it is advisable.
  攻撃の影響を見極め、リスクを低減するための適切な措置を見つけ出すことができるよう、悪意のあるコードの種類を特定する必要性を強調する。ラン

サムウェア攻撃が成功しバックアップがない場合、「no more ransome（ノーモアランサム）」（nomoreransom.org）プロジェクトが提供するものなどの利用可能なツールをデータの復旧に適用できる場合がある。しかし、安全なバックアップが利用できる場合はそこからデータを復元することが望ましい。

- Forwarding or replication all logs to a central log server (possibly including the signing or cryptographic time-stamping of log entries).
  全てのログを中央管理のログサーバーに転送又は複製する（可能であればログエントリの署名又は暗号化されたタイムスタンプを含む）。
- Strong encryption and multi factor authentication, in particular for administrative access to IT systems, appropriate key and password management.
  強力な暗号化及び多要素認証、特に IT システムへの管理アクセスには、適切な鍵管理及びパスワード管理。
- Vulnerability and penetration testing on a regular basis.
  定期的な脆弱性診断及びペネトレーションテスト。
- Establish a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) within the organization, or join a collective CSIRT/CERT. Create an Incident Response Plan, Disaster Recovery Plan and a Business Continuity Plan, and make sure that these are thoroughly tested.
  組織内にコンピュータセキュリティインシデント対応チーム（CSIRT）若しくはコンピュータ緊急対応チーム（CERT）を設置する、又は共同 CSIRT／CERT に参加する。インシデント対応計画、災害復旧計画及び事業継続計画を策定し、それらが徹底的にテストされるよう確保する。
- When assessing countermeasures – risk analysis should be reviewed, tested and updated.
  対応策の評価を実施する際は、リスク分析を見直し、テストし、更新する。

3 DATA EXFILTRATION ATTACKS
3 データを窃取する攻撃

50. Attacks that exploit vulnerabilities in services offered by the controller to third parties over the internet, e.g. committed by way of injection attacks (e.g. SQL injection, path traversal), website compromising and similar methods, may resemble ransomware attacks in that the risk emanates from the action of an unauthorized third party, but those attacks typically aim at copying, exfiltrating and abusing personal data for some malicious end. Hence, they are mainly breaches of confidentiality and, possibly, also data integrity. At the same time, if the controller is aware of the characteristics of this kind of breaches, there are many measures available to controllers that can substantially reduce the risk of a successful execution of an attack.
    管理者がインターネット上で第三者に提供するサービスにおける脆弱性を利用する攻撃、例えば、インジェクション攻撃（SQL インジェクション攻撃、パストラバーサル攻撃、等）、ウェブサイトへの不正アクセス及び同様の手法による攻撃は、無権限の第三者の行為から生じるリスクという点でランサムウェア攻撃に似ているかもしれないが、当該攻撃は通常何らかの悪質な目的のために、個人データを複製、窃取及び悪用することを狙いとしている。ゆえに、当該攻撃は、主にデータの機密性の侵害であり、場合によってはデータの完全性の侵害にもなる。同時に、管理者がこの種の侵害の特徴を認識している場合、攻撃が成功するリスクを大幅に低減することが可能な、管理者が利用できる様々な措置がある。

3.1 CASE No. 05: Exfiltration of job application data from a website
3.1 事例 No.05：ウェブサイトからの求職申込書データの窃取

An employment agency was the victim of a cyber-attack, which placed a malicious code on its website. This malicious code made personal information submitted through online job application forms and stored on the webserver accessible to unauthorized person(s). 213 such forms are possibly affected, after analysing the affected data it was determined that no special categories of data were affected in the breach. The particular malware toolkit installed had functionalities that allowed the attacker to remove any history of exfiltration and also allowed processing on the server to be monitored and to have personal data captured. The toolkit was discovered only a month after its installation.

ある人材派遣会社がサイバー攻撃の標的となり、悪意のあるコードが同社のウェブサイト上に埋め込まれた。この悪意のあるコードは、オンライン上の求職申込フォームを通じて提出され、ウェブサーバー上に保存される個人情報を、無権限の人物に対しアクセスを可能にするものであった。213 の当該応募フォームが影響を受けた可能性があるが、影響を受けたデータの分析の結果、特別な種類のデータは侵害の影響を受けていないと判断された。インストールされたこの特定のマルウェアツールキットには、攻撃者が窃取の履歴を削除できる機能があり、またサーバー上の処理を監視して個人データを取得できる機能もあった。当該ツールキットはインストールされてから 1 カ月後にようやく発見された。

3.1.1 CASE No. 05 - Prior measures and risk assessment
3.1.1 事例 No.05—事前対策及びリスク評価

51. The security of the data controller's environment is extremely important, as the majority of these breaches can be prevented by ensuring that all systems are constantly updated, sensitive data is encrypted and applications are developed according to high security standards like strong authentication, measures against brute force, attacks, "escaping" or "sanitising"[18] user inputs, etc. Periodic IT security audits, vulnerability assessments and penetration tests are also required in order to detect these kinds of vulnerabilities in advance and fix them. In this particular case, file integrity monitoring tools in production environment might have helped to detect the code injection. (A list of advisable measures is to be found in section 3.7).

このような侵害の大半は、全てのシステムの常時更新、センシティブデータの暗号化、及び強力な認証、ブルートフォース攻撃対策、ユーザー入力の「エスケープ」又は「サニタイジング」[18] などといった高度なセキュリティ基準に基づくアプリケーションの開発を確保することにより防止可能なため、データ管理者の環境の安全性は極めて重要である。こうした種類の脆弱性を事前に検知し、修正するため、定期的な IT のセキュリティ監査、脆弱性診断、及びペネトレーションテストも必要である。この特定の事例の場合、本番環境におけるファイルの整合性を監視するツールが悪質なコードの埋込みの検知に役立ったかもしれない（望ましい措置のリストについては本ガイドライン第 3.7 節※を参照）。

※仮訳者注：望ましい措置のリストは、第 3.4 節に説明がある。当該ガイドライ

[18] Escaping or sanitizing user inputs is a form of input validation, which ensures that only properly formatted data is entered into an information system.

ユーザー入力のエスケープ又はサニタイジングとは、入力値の妥当性検証の形式一つであり、正しい書式のデータのみが情報システムに入力されるよう確保するものである。

ン内には第 3.7 節は存在せず、ここでは第 3.4 節を言及しているものと考えられる。

52. The controller should always start to investigate the breach by identifying the type of the attack and its methods, in order to assess what measures are to be taken. To make it fast and efficient, the data controller should have an incident response plan in place which specifies the swift and necessary steps to take control over the incident. In this particular case, the type of the breach was a risk enhancing factor since not only was data confidentiality curtailed, the infiltrator also had the means to establish changes in the system, so data integrity also became questionable.
管理者は、どのような措置をとるべきかを評価するために、侵害の調査を始める際は常に、まず攻撃の種類及びその方法を特定することから始めなければならない。これを素早く効率的に行うために管理者は、インシデントを制御するために取るべく迅速かつ必要な手だてを明記したインシデント対応計画を確立しておかなければならない。この特定の事例では、データの機密性が損なわれただけでなく、侵入者がシステム内を変更する方法も有していたことによりデータの完全性についても疑われたため、侵害の種類がリスクを高める要素となった。

53. The nature, sensitivity and volume of personal data affected in the breach should be assessed to determine to what extent the breach affected the data subjects. Though no special categories of personal data were affected, the accessed data contains considerable information about the individuals from the online forms, and such data could be misused in a number of ways (targeting with unsolicited marketing, identity theft, etc.), so the severity of the consequences should increase the risk to the rights and freedoms of the data subjects[19].
侵害がデータ主体に及ぼした影響の程度を判断するため、侵害により影響を受けた個人データの性質、機微性及び量を評価しなければならない。特別な種類の個人データは影響を受けていないが、アクセスされたデータにはオンラインフォームからの相当量の個人に関する情報が含まれており、そのようなデータは多様な方法で悪用される可能性があるため（未承諾マーケティング、ID 盗取等）、当該影響の深刻度によりデータ主体の権利及び自由に対するリスクは当然増大する [19]。

3.1.2 CASE No. 05 – Mitigation and obligations
3.1.2 事例 No.05—リスク低減措置及び義務

54. If possible, after solving the problem, the database should be compared with the one stored in a secure backup. The experiences drawn from the breach should be utilized in updating the IT infrastructure. The data controller should return all affected IT systems to a known clean state, remedy the vulnerability and implement new security measures to avoid similar data breaches in the future, e.g. file integrity checks and security audits. If personal data was not only exfiltrated, but also deleted, the controller has to take systematic action to recover the personal data in the state it was in before the breach. It may be necessary to apply full backups, incremental changes and then possibly rerun the processing since the last incremental backup – which requires that the controller is able to replicate the changes made since the last backup. This could require that the controller has the system designed to retain the daily input files in case they need to be processed again and requires a robust method of storage and a suitable retention policy.
可能であれば、問題解決後に、データベースを安全なバックアップに保存されて

[19] For guidance on “likely to result in high risk” processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

いるものと比較するべきである。当該侵害から得られた経験を IT インフラの更新に活かさなければならない。データ管理者は、影響を受けた全ての IT システムを元のクリーンな状態に戻し、脆弱性を修正し、今後同様のデータ侵害の発生を防止するための新たな安全管理措置、例えば、ファイルの整合性の確認及びセキュリティ監査を実装しなければならない。個人データが窃取されただけでなく消去された場合、管理者は、個人データを侵害前の状態に復元するために、体系的な行動をとらなければならない。フルバックアップの適用、増分変化の適用、そして次に、可能であれば最後の増分バックアップ以降の処理状態に戻すことが必要になりうる。この場合、管理者が最後のバックアップ以降の変更を再現できる必要がある。これには、管理者が再度処理する必要がある場合に備えて日次入力ファイルを保持するよう設計されたシステムを備えることが必要である可能性があり、またこのためには強固な保存方法及び適切な保持方針が要求される。

55. In light of the above, as the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects should definitely be informed about it (Article 34(1)), which of course means that the relevant SA(s) should also be involved in the form of a data breach notification. Documenting the breach is obligatory according to Article 33 (5) GDPR and makes the assessment of the situation easier.
上記を踏まえ、この侵害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ため、データ主体は確実に当該侵害について連絡を受けなければならず（GDPR 第 34 条第 1 項）、このことは当然、関連する SA もデータ侵害通知という形式で関わってくることを意味する。GDPR 第 33 条第 5 項に基づく侵害の文書化は義務であり、また文書化をすることは状況の評価を容易にする。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

3.2 CASE No. 06: Exfiltration of hashed password from a website
3.2 事例 No.06：ウェブサイトからのハッシュ化されたパスワードの窃取

An SQL Injection vulnerability was exploited to gain access to a database of the server of a cooking website. Users were only allowed to choose arbitrary pseudonyms as usernames. The use of email addresses for this purpose was discouraged. Passwords stored in the database were hashed with a strong algorithm and the salt was not compromised. Affected data: hashed passwords of 1.200 users. For safety's sake, the controller informed the data subjects about the breach via e-mail and asked them to change their passwords, especially if the same password was used for other services.
SQL インジェクションの脆弱性が悪用され、ある料理サイトのサーバー上のデータベースがアクセスされた。ユーザーはユーザー名として任意の仮名を選択することのみ許されていた。この目的に電子メールアドレスを使用することは推奨されていなかった。データベースに保存されたパスワードは強力なアルゴリズムによりハッシュ化されており、そのソルトへの不正アクセスはなかった。影響を受けたデータは、ユーザー1,200 名分のハッシュ化されたパスワード。安全のため、管理者はデータ主体に対し、電子メールを通じて侵害を通知し、特に同一のパスワードを他のサービスに使用している場合、パスワードを変更するよう求めた。

3.2.1 CASE No. 06 - Prior measures and risk assessment
3.2.1 事例 No.06—事前対策及びリスク評価

56. In this particular case data confidentiality is compromised, but the passwords in the database were hashed with an up-to-date method, which would decrease the risk regarding the nature, sensitivity, and volume of personal data. This case presents no risks to the rights and freedoms of the data subjects.
この特定の事例では、データの機密性が侵害されているが、データベース内のパスワードは最新の手法によりハッシュ化されており、このことが個人データの性質、機微性及び量に関するリスクを低下させる。この事例は、データ主体の権利及び自由に対するリスクをもたらすものではない。

57. Furthermore, no contact information (e.g. e-mail addresses or phone numbers) of data subjects was compromised, which means there is no significant risk for the data subjects of being targeted by fraud attempts (e.g. receiving phishing e-mails or fraudulent text messages and phone calls). No special categories of personal data were involved.
さらに、データ主体の連絡先情報（電子メールアドレス又は電話番号等）への不正アクセスはなく、このことは、データ主体が詐欺の試みの標的となる（フィッシングメール又は詐欺のテキストメッセージや詐欺電話を受ける、等）ような重大なリスクはないことを意味する。特別な種類の個人データは含まれていない。

58. Some user names could be regarded as personal data, but the subject of the website does not allow for negative connotations. Although it has to be noted that the risk assessment may change[20], if the type of the website and the data accessed could reveal special categories of personal data (e. g. website of a political party or trade union). Using state of the art encryption could mitigate the adverse effects of the breach. Assuring that a limited number of attempts to login is allowed will prevent brute force login attacks to be successful, thus reducing largely the risks imposed by attackers already knowing the usernames.
一部のユーザー名は個人データとみなされる可能性があろうが、当該ウェブサイトの主題はネガティブな意味合いを持つ余地はない。一方、ウェブサイトの種類及びアクセスされたデータが特別な種類の個人データを明らかにする可能性がある場合（政党又は労働組合のウェブサイト、等）、リスク評価が変わりうることに注意しなければならない [20]。最新の暗号化を使用することにより、侵害の悪影響が低減される可能性がある。ログイン試行回数の制限を確保することは、ブルートフォースのログイン攻撃の成功を防止し、よってユーザーネームを既に知っている攻撃者がもたらすリスクを大幅に減らす。

3.2.2 CASE No. 06 – Mitigation and obligations
3.2.2 事例 No.06—リスク低減措置及び義務

59. The communication to the data subjects in some cases could be considered a mitigating factor, since the data subjects are also in a position to make the necessary steps to avoid further damages from the breach, for example by changing their password. In this case, notification was not mandatory, but in many cases it can be considered a good practice.
データ主体も侵害による更なる損害を避けるために必要な手だて、例えば、パスワード変更等を講じることができるため、場合によっては、データ主体へ連絡することがリスクを低減する要素の一つとみなすことができるであろう。今回の事例では連絡は義務ではないが、多くのケースにおいて望ましい慣行とみなすことができる。

[20] For guidance on “likely to result in high risk” processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

60. The data controller should correct the vulnerability and implement new security measures to avoid similar data breaches in the future like, for example, systematic security audits to the website.
データ管理者は脆弱性を修正し、今後同様のデータ侵害の発生を防止するため、例えばウェブサイトに対する体系的なセキュリティ監査のような、新たな安全管理措置を実装しなければならない。

61. The breach should be documented in accordance with Article 33 (5) but no notification or communication needed.
この侵害は、GDPR 第 33 条第 5 項に基づき文書化しなければならないが、通知又は連絡は要求されない。

62. Also, it is strongly advisable to communicate a breach involving passwords to data subjects in any case even when the passwords were stored using a salted hash with an algorithm conforming to the state-of-the-art. The use of authentication methods obviating the need to process passwords on the server side is preferable. Data subjects should be given the choice to take appropriate measures regarding their own passwords.
また、パスワードに関わる侵害をデータ主体に連絡することは、いかなる場合でも、たとえパスワードが最新のアルゴリズムによるソルト付きのハッシュを用いて保存されていた場合であったとしても、強く望ましい措置である。サーバー側でパスワードを処理する必要性を回避する認証方式の使用がより望ましい。データ主体に対し、自らのパスワードについて適切な措置をとれるような選択肢を与えるべきである。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

3.3 CASE No. 07: Credential stuffing attack on a banking website
3.3 事例 No.07：バンキングサイトへのクレデンシャルスタッフィング攻撃

A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose

data was disclosed.

ある銀行のオンラインバンキングサイトの1つが、サイバー攻撃を受けた。当該攻撃は、ある決まり切った一般的なパスワードを使いログイン可能な全てのユーザーID を列挙することを目的としていた。パスワードは 8 桁で構成されている。ウェブサイトの脆弱性により、使用されたパスワードが正しくない又は銀行口座が既に使われていないにもかかわらず、データ主体に関する情報（氏名、性別、生年月日、出生地、納税者番号、ユーザーID 番号）が攻撃者に漏洩した場合もあった。これにより、約 10 万人のデータ主体が影響を受けた。攻撃者は、うち、当該攻撃者が試した一般的なパスワードを使用していた約 2,000 人分のアカウントへのログインに成功した。事件後、管理者は全ての不正なログイン試行を特定することが出来た。管理者は、不正防止確認により、攻撃中これらのアカウントにおいて取引がなかったことを確認できた。銀行は、セキュリティオペレーションセンターが当該ウェブサイトに対し大量のログイン要求を検知したことにより、当該データ侵害を認識した。管理者はこれに対応して、ログインの停止によりウェブサイトへのログインを不可能にし、不正アクセスされたアカウントのパスワードを強制リセットした。管理者は不正アクセスされた、例えば、パスワードが侵害を受けた又はデータが漏洩したアカウントのユーザーにのみ侵害を連絡した。

3.3.1 CASE No. 07 - Prior measures and risk assessment
3.3.1 事例 No.07—事前対策及びリスク評価

63. It is important to mention that controllers handling data of highly personal nature[21] have a larger responsibility in terms of providing adequate data security, e.g. having a security operation's centre and other incident prevention, detection and response measures. Not meeting these higher standards will certainly result in more serious measures during an SA's investigation.
極めて個人的な性質のデータ [21] を取扱う場合、管理者は十分なデータの安全性を提供すること、例えば、セキュリティオペレーションセンターの設置、その他のインシデントの防止、検知及び対応のための措置を講じることについて、より重大な責任を負うということに言及することが重要である。これらのようなより高い基準を満たしていない場合、SA の調査において明らかにより厳しい措置が取られる。

64. The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high.
この侵害は身元情報及びユーザーID 情報のみならず財務データに関わるため、特に深刻なものになる。影響を受ける個人の数は多い。

65. The fact that a breach could happen in such a sensitive environment points to significant data security holes in the controller's system, and may be an indicator of a time when the review and update of affected measures is "necessary" in line with Articles 24 (1), 25 (1), and 32 (1) of the GDPR. The breached data permits the unique identification of data subjects and contains other information about them (including gender, date and place of birth), furthermore it can be used by the attacker to guess the customers' passwords or to

[21] Such as information of the data subjects referred to payment methods such as card numbers, bank accounts, online payment, payrolls, bank statements, economic studies or any other information that may reveal economic information pertaining to the data subjects.
データ主体のカード番号、銀行口座、オンライン支払、給与、銀行取引明細書、経済性の調査、又はその他データ主体に関する経済性の情報を開示しうる情報等、支払方法に参照されるデータ主体の情報といったもの。

run a spear phishing campaign directed at the bank customers.
このようなセンシティブな環境において侵害が生じうるという事実は、管理者のシステム内に重大なデータのセキュリティホールが存在することを示し、GDPR 第 24 条第 1 項、第 25 条第 1 項及び第 32 条第 1 項に従い、影響を受けた措置の見直し及び更新がいつ「必要」かの時間の指標となりうる。今回侵害されたデータは、データ主体を一意に識別することを可能にするものである。またデータ主体に関する他の情報（性別、生年月日及び出生地等）を含んでおり、当該情報は更に攻撃者により、顧客のパスワードの推測又は当該銀行の顧客を狙ったスピアフィッシング攻撃に利用される可能性がある。

66. For these reasons, the data breach was deemed likely to result in a high risk to the rights and freedoms of all the data subjects concerned[22]. Therefore, the occurrence of material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud) is a conceivable outcome.
これらの理由により、当該データ侵害は関係する全てのデータ主体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とみなされた [22]。従って、財産的な損失（金銭的損失等）及び非財産的な損失（ID 盗取又は ID 詐欺等）の発生は、考えられる結果である。

3.3.2 CASE No. 07 – Mitigation and obligations
3.3.2 事例 No.07—リスク低減措置及び義務

67. The controller's measures mentioned in the case description are adequate. In the wake of the breach it also corrected the vulnerability of the website and took other steps to prevent similar future data breaches, such as adding two-factor authentication to the concerned website and moving up to a strong customer authentication.
事例説明で言及されている管理者の措置は妥当である。侵害を受け管理者はまた、ウェブサイトの脆弱性を修正し、例えば当該侵害を受けたウェブサイトへの二要素認証の追加及び強力な顧客認証への移行といった、今後同様のデータ侵害の発生を防止するための他の手だても講じた。

68. Documenting the breach according to Article 33 (5) GDPR and notifying the SA about it are not optional in this scenario. Furthermore, the controller should notify all 100.000 data subjects (including the data subjects whose accounts were not compromised) in accordance with Article 34 GDPR.
この事例では、GDPR 第 33 条第 5 項に基づく侵害の文書化及び SA に対する通知が必須である。加えて管理者は、GDPR 第 34 条に基づき 10 万人全てのデータ主体（アカウントへの不正アクセスがなかったデータ主体を含む）に対し通知しなければならない。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

[22] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

3.4 Organizational and technical measures for preventing / mitigating the impacts of hacker attacks
3.4 ハッカー攻撃の防止／影響低減のための組織的及び技術的な措置

69. Just as in case of ransomware attacks, regardless of the outcome and the consequences of the attack, re-evaluating IT security is compulsory for controllers in similar cases.
ランサムウェア攻撃の場合と同様、攻撃の結果と影響にかかわらず、同様のケースにおける管理者にとって、IT セキュリティの再評価は必須である。

70. Advisable measures:[23]
望ましい措置 [23]

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most*.)
（下記の措置のリストは、これ以外の措置を排除するものでも全てを網羅するものでもない。むしろ防止案及び考えられる解決策の提供を目的とするものである。取扱活動はそれぞれ異なるため、管理者は状況に応じて最適な措置を決定しなければならない。）

- State-of-the-art encryption and key management, especially when passwords, sensitive or financial data are being processed. Cryptographic hashing and salting for secret information (passwords) is always preferred over encryption of passwords. The use of authentication methods obviating the need to process passwords on the server side is preferable.
最新の暗号化及び鍵管理、特にパスワード、センシティブデータ又は財務データが取扱われる場合。秘密情報（パスワード）には、パスワードの暗号化よりも暗号学的ハッシュとソルトが常に望ましい。サーバー側でパスワードを処理する必要のない認証方法の使用がより望ましい。
- Keeping the system up to date (software and firmware). Ensuring that all IT security measures are in place, making sure they are effective and keeping them regularly updated when processing or circumstances change or evolve. In order to be able to demonstrate compliance with Article 5(1)(f) in accordance with Article 5 (2) GDPR the controller should maintain a record of all updates performed, including also the time when they were applied.
システムを最新の状態に維持する（ソフトウェア及びファームウェア）。全ての IT の安全管理措置を設けることを確保し、それらを確実に有効な状態にし、取扱い若しくは状況に変更又は展開がある際は常に更新することを維持する。管理者は、GDPR 第 5 条第 2 項に基づき第 5 条第 1 項(f)の順守を証明できるよう、実行した全ての更新について、適用された時間も含め、記録を保持しなければならない。
- Use of strong authentication methods like two-factor authentication and authentication servers, complemented by an up-to-date password policy.
二要素認証及び認証サーバーのような強力な認証方法を使用し、これを最新のパスワード方針により補完する。
- Secure development standards include the filtering of user input (using white listing as

[23] For secure web application development see also: https://www.owasp.org/index.php/Main_Page .
安全なウェブアプリケーションの開発については次も参照：
https://www.owasp.org/index.php/Main_Page

far as practicable), escaping user inputs and brute force prevention measures (such as limiting the maximum amount of retries). “Web Application Firewalls” may assist in the effective use of this technique.
ユーザー入力のフィルタリング（実行可能な限りでホワイトリストを使用）、ユーザー入力のエスケープ及びブルートフォース攻撃防止措置（再入力の最大回数を制限する、等）を含む安全な開発基準。この技術の効果的な使用については、「ウェブアプリケーションファイアウォール」が役立ちうる。

- Strong user privileges and access control management policy in place.
  強力なユーザー権限及びアクセス管理の管理方針を設ける。
- Use of appropriate, up-to-date, effective and integrated firewall, intrusion detection and other perimeter defence systems.
  適切で、最新の、有効で、かつ統合されたファイアウォール、侵入検知システム、及びその他の境界防御システムの使用。
- Systematic IT security audits and vulnerability assessments (penetration testing).
  体系的な IT のセキュリティ監査及び脆弱性診断（ペネトレーションテスト）。
- Regular reviews and testing to ensure that backups can be used to restore any data whose integrity or availability was affected.
  完全性又は可用性が影響を受けたデータを復元するために、バックアップが使用できるよう確保するために、定期的な見直し及びテストを実施する。
- No session ID in URL in plain text.
  セッション ID を URL 内に平文で記述しない。

4 INTERNAL HUMAN RISK SOURCE
4 内部の人的なリスク源

71. The role of human error in personal data breaches has to be highlighted, due to its common appearance. Since these types of breaches can be both intentional and unintentional, it is very hard for the data controllers to identify the vulnerabilities and adopt measures to avoid them. The International Conference of Data Protection and Privacy Commissioners recognized the importance of addressing such human factors and adopted the resolution to address the role of human error in personal data breaches in October 2019[24]. This resolution stresses that appropriate safeguarding measures should be taken to prevent human errors and provides a non-exhaustive list of such safeguards and approaches.
個人データ侵害の中でも、よく生じるという理由から、ヒューマンエラーによるものを重視する必要がある。この種類の侵害は意図的な場合及び意図的でない場合の両方がありえ、データ管理者にとって脆弱性を特定し、この種の侵害を防止する措置を講じることは非常に困難である。データ保護プライバシー・コミッショナー国際会議は、そのような人的な要因に対処することの重要性を認識し、2019 年 10 月、個人データ侵害におけるヒューマンエラーによるものに対処するための決議を採択した [24]。当該決議は、ヒューマンエラーの防止のために適切な保護措置が講じられるべきであることを強調し、そのような保護措置及びアプローチの非包括的なリストを提供している。

4.1 CASE No. 08: Exfiltration of business data by an employee
4.1 事例 No.08：従業員によるビジネス上のデータの窃取

During his period of notice, the employee of a company copies business data from the

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

company's database. The employee is authorized to access the data only to fulfill his job tasks. Months later, after quitting the job, he uses the data thus gained (basic contact data) to feed a new data processing for which he is the controller in order to contact the clients of the company to entice them to his new business.
ある会社の従業員が、退職通知期間中に会社のデータベースからビジネス上のデータを複製する。当該従業員には、職務遂行のためにのみ当該データへのアクセス権限がある。数カ月後、退職した後、当該従業員はその際得たデータ（顧客の基本的な連絡先データ）を使用し、自身の新規事業へ勧誘するため退職した会社の顧客へ連絡することを目的として、自らが管理者となる新規のデータ取扱いを入力する。

4.1.1 CASE No. 08 - Prior measures and risk assessment
4.1.1 事例 No.08—事前対策及びリスク評価

72. In this particular case no prior measures were taken to prevent the employee from copying contact information of the company's clientele, since he needed – and had – legitimate access to this information for his job tasks. Since fulfilling most customer relation jobs require some kind of access to personal data, these data breaches may be the most difficult to prevent. Limitations to the scope of access may limit the work the given employee is able to do. However, well thought out access policies and constant control can help prevent such breaches.
この特定の事例では、当該従業員は職務のために当該情報へのアクセス権限が必要であり、また保持していたため、当該従業員が会社の顧客の連絡先情報を複製することについて、防止するための事前の対策は講じられていなかった。ほとんどの顧客関連の業務は、遂行するうえで何らかの個人データへのアクセスを要することから、このようなデータ侵害は最も防止が難しいかもしれない。アクセスの範囲を制限することは、該当の従業員が遂行可能な業務を制限しうる。しかし、綿密なアクセス方針及び常時のアクセス管理を維持することが、こうした侵害の防止に役立ちうる。

73. As usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration. These kinds of breaches are typically breaches of confidentiality, since the database is usually left intact, its content "merely" copied for further use. The quantity of data affected is usually also low or medium. In this particular case no special categories of personal data were affected, the employee only needed the contact information of clients to enable him to get in touch with them after leaving the company. Therefore, the data concerned is not sensitive.
このケースにおいても同様に、リスク評価において、侵害の種類並びに影響を受けた個人データの性質、機微性及び量を考慮に入れなければならない。この手の侵害は、データベースは通常影響を受けず、その後の使用のためにその内容を「単に」複製されるのみであるため、一般的に機密性の侵害となる。影響を受けるデータの量も通常、少数又は中程度である。この特定の事例では、特別な種類の個人データは影響を受けておらず、当該従業員は退職後に連絡を取るために顧客の連絡先情報を必要としたのみであった。従って、関係するデータはセンシティブなものではない。

74. Although the only goal of the ex-employee that maliciously copied the data may be limited to gaining the contact information of the company's clientele for his own commercial purposes, the controller is not in a position to consider the risk for the affected data subjects to be low, since the controller does not have any kind of reassurance on the intentions of the employee. Thus, while the consequences of the breach might be limited

to the exposure to uncalled-for self-marketing of the ex-employee, further and more grave abuse of the stolen data is not ruled out, depending on the purpose of the processing put in place by the ex- employee[25].

悪意を持ってデータの複製を作成した元従業員の唯一の目的は、自らの事業目的のために会社の顧客の連絡先情報を得ることに限定されるかもしれないが、管理者は元従業員の意図についていかなる確証もないため、当該管理者は影響を受けるデータ主体のリスクが低いとみなす立場にはない。従って、この侵害の影響は、元従業員による不必要な勧誘にさらされることのみに留まるかもしれないが、当該元従業員が設定した取扱いの目的次第では、盗まれたデータの追加的な、より深刻な悪用が排除されない[25]。

4.1.2 CASE No. 08 – Mitigation and obligations
4.1.2 事例 No.08—リスク低減措置及び義務

75. The mitigation of the adverse effects of the breach in the above case is difficult. It might need to involve immediate legal action to prevent the former employee from abusing and disseminating the data any further. As a next step, the avoidance of similar future situations should be the goal. The controller might try to order the ex-employee to stop using the data, but the success of this action is dubious at best. Appropriate technical measures such as the impossibility of copying or downloading data to removable devices may help.

上記の事例での侵害の悪影響を低減することは困難である。元従業員によるデータの追加的な悪用及び拡散を防ぐため、直ちに法的措置をとる必要があるかもしれない。次の手だてとして、今後同様の事態が発生することを防止しなければならない。管理者は元従業員に対し、データの使用を停止するよう命令を試みるかもしれないが、この行動が成功するかは最善を尽くしても疑わしい。取外し可能なデバイスへのデータの複製又はダウンロードを不可能にするなどの適切な技術的措置が役立ちうる。

76. There is no “one-size fits-all” solution to these kinds of cases, but a systematic approach may help to prevent them. For example, the company may consider – when possible - withdrawing certain forms of access from employees who have signalled their intention to quit or implementing access logs so that unwanted access can be logged and flagged. The contract signed with employees should include clauses that prohibit such actions.

この種のケースに対する「万能の」解決法はないが、体系的なアプローチが防止に役立ちうる。例えば、会社は、可能な場合には、退職の意向を示した従業員について一定の形式のアクセスを取消す、又は不必要なアクセスを記録しフラグを立てられるようアクセスログを実装することを検討しうる。従業員と締結する契約に、こうした行為を禁止する条項を盛込む必要がある。

77. All in all, as the given breach will not result in a high risk to the rights and freedoms of natural persons, a notification to the SA will suffice. However, the information to the data subjects might be beneficial for the data controller too, since it might be better that they hear from the company about the data leak rather than from the ex-employee who tries to contact them. Data breach documentation in accordance with Article 33 (5) is a legal obligation.

概して、今回の侵害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ものではないため、SA に対する通知で十分である。しかし、データ主体が連絡を試

[25] For guidance on “*likely to result in high risk*” processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

みる元従業員から連絡を受けるより、会社からデータ漏洩について連絡を受ける方がよいと考えられるため、データ主体に対する連絡はデータ管理者にとっても有益であろう。GDPR 第 33 条第 5 項に基づくデータ侵害の文書化は法的義務である。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	X

4.2 CASE No. 09: Accidental transmission of data to a trusted third party
4.2 事例 No.09：信頼された第三者に対するデータの偶発的な送付

An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the breach.

ある保険代理店が、電子メールで受信したエクセルファイルの設定の誤りにより、当該代理店の担当範囲に属さない二十数名分の顧客に関わる情報にアクセスできることに気づいた。当該代理店は職務上の守秘義務を負っており、また当該電子メールの唯一の受取人であった。データ管理者と当該代理店との取決めにより、当該代理店は個人データの侵害をデータ管理者に対し不当に遅滞なく通知することが義務付けられている。従って、当該代理店は誤りについて直ちに管理者に通知した。管理者はファイルを修正のうえ再送し、当該代理店に対し先に送ったメッセージの消去を求めた。上記の取決めでは、当該代理店はその消去について、書面による声明で確認する必要があり、その通りに実施した。取得された情報には、特別な種類の個人データは含まれておらず、連絡先データ及び保険そのものについての情報（保険の種類、金額）のみ含まれている。当該侵害の影響を受けた個人データの分析を行った結果、データ管理者は、個人側にも又はデータ管理者側にも、侵害の深刻度に影響しうるいかなる特別な特性も確認しなかった。

4.2.1 CASE No. 09 – Prior measures and risk assessment
4.2.1 事例 No.09—事前対策及びリスク評価

78. Here the breach does not derive from an intentional action of an employee, but from an unintentional human error caused by inattentiveness. These kinds of breaches may be avoided or decreased in frequency by a) enforcing training, education and awareness

programs where employees gain a better understanding of the importance of personal data protection, b) reducing file exchange through e-mail, instead using dedicated systems for processing customer data for example, c) double checking files before sending, d) separating the creation and sending of files.
ここでは、侵害は従業員の意図的な行動から生じておらず、不注意が原因の意図的ではないヒューマンエラーによるものである。このような侵害は以下の対策により防止又は頻度の削減が可能である。a）従業員が個人データ保護の重要性をよりよく理解するための訓練、教育及び意識向上プログラムを実施する、b）電子メールを通じたファイル交換を減らし、代わりに例えば顧客データ処理専用のシステムを使用する、c）送信前にファイルのダブルチェックを行う、d）ファイルの作成と送信を分ける。

79. This data breach concerns only the confidentiality of the data, and the integrity and the accessibility thereof are left intact. The data breach only concerned about two dozen costumers, hence the quantity of data affected can be considered as low. Furthermore, the personal data affected does not contain any sensitive data. The fact that the data processor immediately contacted the data controller after becoming aware of the data breach can be considered a risk mitigating factor. (The possibility of data having been sent to other insurance agents should also be evaluated and, if confirmed, proper measures should be taken.) Due to the appropriate steps taken after the data breach, it will probably not have any impact on the data subjects' rights and freedoms.
今回のデータ侵害はデータの機密性にのみ関わるものであり、従って、データの完全性及びアクセス可能性には影響がない。当該侵害は約二十名の顧客のみに関わるものであり、従って影響を受けたデータの量は少ないとみなすことができる。更に、今回影響を受けた個人データにはいかなるセンシティブデータも含まれていない。当該侵害に気づいたデータ処理者が直ちにデータ管理者に連絡した事実は、リスク低減要素の一つと見なすことができる。（データが他の保険代理店に送信された可能性についても評価する必要があり、確認された場合は適正な手だてを講じなければならない。）データ侵害後に適切な措置が取られたため、今回の侵害によるデータ主体の権利及び自由に対する影響は恐らくない。

80. The combination of the low number of individuals affected, the immediate detection of the breach and the measures taken to have its effects minimized make this particular case no risk.
影響を受けた個人が少数であること、直ちに侵害を検知したこと、及び影響を最小限にとどめる措置を講じたことの組合わせにより、この特定の事例はリスクがないものとなる。

4.2.2 CASE No. 09 – Mitigation and obligations
4.2.2 事例 No.09—リスク低減措置及び義務

81. Moreover, other risk mitigating circumstances are at play as well: the agent is bound by professional secrecy; he himself reported the problem to the controller; and he deleted the file upon request. Raising awareness and possibly including additional steps in checking documents involving personal data will probably help avoid similar cases in the future.
加えて、他にもリスクを低減させる状況が作用している。つまり、当該保険代理店は職務上の守秘義務を負っていたこと、自ら管理者に問題を報告したこと、そして要請に応じてファイルを消去したことである。意識の向上と、可能であれば個人データを含む文書を確認する場合に追加的な手だてを加えることが、今後の同様のケースの回避に役立つであろう。

82. Besides documenting the breach in accordance with Article 33 (5), there is no need for any

other action.
GDPR 第 33 条第 5 項に基づく侵害の文書化以外に、他の措置を講じる必要はない。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

4.3 Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources

4.3 内部の人的なリスク源の防止／影響低減のための組織的及び技術的な措置

83. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.
下記の措置を組合せ、ケース毎の特徴に応じて適用することで、同様の侵害の発生の可能性を低下させることに役立つであろう。

84. Advisable measures:
望ましい措置

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下記の措置のリストは、これ以外の措置を排除するものでも全てを網羅するものでもない。むしろ防止案及び考えられる解決策の提供を目的とするものである。取扱活動はそれぞれ異なるため、管理者は状況に応じて最適な措置を決定しなければならない。）

- Periodic implementation of training, education and awareness programs for employees on their privacy and security obligations and the detection and reporting of threats to the security of personal data[26]. Develop an awareness program to remind employees of the most commons errors leading to personal data breaches and how to avoid them.
プライバシー及びセキュリティに関する義務、並びに個人データの安全性への脅威の検知及び通報に関して、従業員を対象とした訓練、教育及び認識プログラムを定期的に実施する [26]。個人データ侵害に繋がる最も一般的なエラー及びその防止策について従業員に認識させるための、意識向上プログラムを開発する。
- Establishment of robust and effective data protection and privacy practices, procedures and systems[27].
強固かつ効果的なデータ保護並びにプライバシーに関する慣行、手順及び体系を確立する [27]。

[26] Section 2) subsection (i) of the Resolution to address the role of human error in personal data breaches.
個人データ侵害におけるヒューマンエラーによるものに対処するための決議 2) (i)
[27] Section 2) subsection (ii) of the Resolution to address the role of human error in personal data breaches.
個人データ侵害におけるヒューマンエラーによるものに対処するための決議 2) (ii)

- Evaluation of privacy practices, procedures and systems to ensure continued effectiveness[28].
  継続的な有効性を確保すべく、プライバシーに関する慣行、手順及び体系の評価を実施する [28]。
- Making proper access control policies and forcing users to follow the rules.
  適正なアクセス管理方針を策定し、ユーザーにルールを順守させる。
- Implementing techniques to force user authentication when accessing sensitive personal data.
  センシティブな個人データへのアクセス時にユーザー認証を強制する技術を実装する。
- Disabling the company related account of the user as soon as the person leaves the company.
  従業員が退職する際直ちに、当該従業員の会社関連のユーザーアカウントを無効化する。
- Checking unusual dataflow between the file server and employee workstations.
  ファイルサーバーと従業員のワークステーション間の、通常と異なるデータの流れを確認する。
- Setting up I/O interface security in the BIOS or through the use of software controlling the use of computer interfaces (lock or unlock e. g. USB/CD/DVD etc.).
  バイオス（BIOS）の出入力インターフェースのセキュリティ設定をする、又はソフトウェアの使用を通じてコンピューターのインターフェースの使用を管理する（USB/CD/DVD 等のロック又はロック解除）。

- Reviewing employees' access policy (e.g. logging access to sensitive data and requiring the user to input a business reason, so that this is available for audits).
  従業員のアクセス方針を見直す（例えば、監査時に提出できるように、センシティブデータへのアクセスを記録し、ユーザーに業務上の理由の入力を求める）。
- Disabling open cloud services.
  オープンソースのクラウドサービスを無効化する。
- Forbidding and preventing access to known open mail services.
  一般に知られているオープンソースのメールサービスへのアクセスを禁止及び阻止する。
- Disabling print screen function in OS.
  OS のスクリーンショット機能を無効化する。
- Enforcing a clean desk policy.
  クリアデスク方針を実施する。
- Automated locking all computers after a certain amount of time of inactivity.
  全てのコンピュータについて、無操作状態で一定時間経過後、自動的にロックする。
- Use mechanisms (e.g. (wireless) token to log on/open locked accounts) for fast user switches in shared environments.
  共有環境においてユーザー切替を迅速に行う仕組み（例えば、ロックされたアカウントにログオン／アクセスするための（無線式の）トークン）を使用する。
- Use of dedicated systems for managing personal data that apply appropriate access

[28] Section 2) subsection (iii) of the Resolution to address the role of human error in personal data breaches.
個人データ侵害におけるヒューマンエラーによるものに対処するための決議 2) (iii)

control mechanisms and that prevent human mistake, such as sending of communications to the wrong subject. The use of spreadsheets and other office documents is not an appropriate means to manage client data.
適切なアクセス管理の仕組みが適用されており、また間違った相手にメールを送るといったようなヒューマンエラーを防止するような個人データ管理専用のシステムを使用する。スプレッドシートやその他のオフィスドキュメントの使用は、顧客データの管理の手段としては適切ではない。

5 LOST OR STOLEN DEVICES AND PAPER DOCUMENTS
5 デバイス及び紙文書の紛失又は盗難

85. A frequent type of case is the loss or theft of portable devices. In these cases, the controller has to take into consideration the circumstances of the processing operation, such as the type of data stored on the device, as well as the supporting assets, and the measures taken prior to the breach to ensure an appropriate level of security. All of these elements affect the potential impacts of the data breach. The risk assessment might be difficult, as the device is no longer available.
よく起きるケースの一つは、携帯型のデバイスの紛失又は盗難である。この場合、管理者は、当該サポートアセット同様、そのデバイスに保存されているデータの種類といった取扱業務の状況、及び適切なセキュリティレベルを確保するために侵害前に講じられていた措置を考慮しなければならない。これらの要素は全て、データ侵害がもたらす可能性のある影響に関係する。デバイスが存在しないため、リスク評価は困難なものとなるかもしれない。

86. These kinds of breaches can be always classified as breaches of confidentiality. However, if there is no backup for the stolen database, then the breach type can also be breach of availability and breach of integrity.
この種の侵害は常に、機密性の侵害に分類される。ただし、盗まれたデータベースのバックアップがない場合、侵害の種類は可用性の侵害及び完全性の侵害にもなりうる。

87. The scenarios bellow demonstrate how the above mentioned circumstances influence the likelihood and severity of the data breach.
下記の事例は、上記の状況がどのようにデータ侵害の蓋然性及び深刻度に影響を及ぼすかについて説明するものである。

5.1 CASE No. 10: Stolen material storing encrypted personal data
5.1 事例 No.10：暗号化された個人データが保存されたデバイスの盗難

During a break-in into a children's day-care centre, two tablets were stolen. The tablets contained an app which held personal data about the children attending the day-care centre. Name, date of birth, personal data about the education of the children were concerned. Both the encrypted tablets which were turned off at the time of the break-in, and the app were protected by a strong password. Back-up data was effectively and readily available to the controller. After becoming aware of the break-in, the day-care remotely issued a command to wipe the tablets shortly after the discovery of the break-in.
ある保育所で、不法侵入の間に、タブレット 2 台が盗まれた。当該タブレットには、保育所に通う児童の個人データが入っているアプリが含まれていた。児童の氏名、生年月日、教育に関する個人データが関わっていた。侵入発生

時に電源が切られていた暗号化されたタブレット及びアプリの両方が強力なパスワードで保護されていた。管理者は、バックアップデータを効果的かつ迅速に使用できた。不法侵入に気づいた後、保育所は、不法侵入の発覚から間を置かずに、遠隔操作によりタブレット内のデータ消去の指示を発行した。

5.1.1 CASE No. 10 - Prior measures and risk assessment
5.1.1 事例 No.10—事前対策及びリスク評価

88. In this particular case the data controller took adequate measures to prevent and mitigate the impacts of a potential data breach by using device encryption, introducing adequate password protection and securing back-up of the data stored on the tablets. (A list of advisable measures is to be found in section 5.7※).
この特定の事例では、データ管理者がデバイスの暗号化を使用し、適切なパスワードによる保護を導入し、またタブレットに保存されているデータのバックアップを確保することで、生じる可能性のあるデータ侵害からの影響を防止し、低減するための適切な措置を講じていた（望ましい措置のリストは本ガイドライン第 5.7 節※参照）。
※仮訳者注：望ましい措置のリストは、第 5.4 節に説明がある。当該ガイドライン内には第 5.7 節は存在せず、ここでは第 5.4 節を言及しているものと考えられる。

89. After becoming aware of a breach, the data controller should assess the risk source, the systems supporting the data processing, the type of personal data involved and the potential impacts of the data breach on the concerned individuals. The data breach described above would have concerned confidentiality, availability and integrity of the concerned data, however due to the appropriate proceedings of the data controller prior and after the data breach none of these occurred.
データ管理者は、侵害に気づいた後、リスク源、データ処理のサポートシステム、関係する個人データの種類、及び関係する個人に対するデータ侵害により生じる可能性のある影響について評価しなければならない。上記の侵害は、関係するデータの機密性、可用性及び完全性に関わる侵害となっていたであろうが、データ管理者がデータ侵害前後に講じた適切な手続きにより、いずれの侵害も起こらなかった。

5.1.2 CASE No. 10 – Mitigation and obligations
5.1.2 事例 No.10—リスク低減措置及び義務

90. The confidentiality of the personal data on the devices was not compromised due to the strong password protection on both the tablets and the apps. The tablets were set up in such a way that setting a password also means that the data on the device is encrypted. This was further enhanced by the controller's action to attempt to remotely wipe everything from the stolen devices.
タブレット及びアプリの両方が強力なパスワードで保護されていたことにより、デバイス上の個人データの機密性は損なわれなかった。タブレットは、パスワードを設定することでデバイス上のデータが暗号化される方法で設定されていた。このことは、遠隔操作により盗まれたデバイスから全データを消去することを試みた管理者の行動により、さらに強化された。

91. Due to the measures taken, the confidentiality of the data was kept intact too. Furthermore, the backup ensured the continuous availability of the personal data, hence no potential negative impact could have occurred.
講じられた措置によっても、データの機密性は損なわれなかった。さらに、バッ

クアップにより個人データの継続的な可用性が確保されたため、起こり得た悪影響は生じなかった。

92. Due to these facts, the above described data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33 (5).
これらの事実から、上記のデータ侵害はデータ主体の権利及び自由に対するリスクを発生させるおそれはなく、従って SA 又は関係するデータ主体に対する通知は必要ない。しかしながら、当該データ侵害も GDPR 第 33 条第 5 項に基づく文書化はしなければならない。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

5.2 CASE No. 11: Stolen material storing non-encrypted personal data
5.2 事例 No.11：暗号化されていない個人データが保存されたデバイスの盗難

The electronic notebook device of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers. Due to the unavailability of the stolen device it was not possible to identify if other categories of personal data were also affected. The access to the notebook's hard drive was not protected by any password. Personal data could be restored from daily backups available.
あるサービス提供会社の従業員の電子手帳機器が盗まれた。当該盗まれた電子手帳には、顧客 10 万人以上の名前、姓、性別、住所及び生年月日が入っていた。盗まれたデバイスが存在しないため、他の種類の個人データについても影響があるかについては特定できなかった。当該電子手帳のハードドライブへのアクセスについて、パスワードによる保護が一切されていなかった。個人データは利用可能な日次バックアップから復元可能である。

5.2.1 CASE No. 11 - Prior measures and risk assessment
5.2.1 事例 No.11—事前対策及びリスク評価

93. No prior safety measures were taken by the data controller, hence the personal data stored on the stolen notebook was easily accessible for the thief or any other person coming into possession of the device thereafter.
データ管理者が事前の安全管理措置を講じていなかったため、盗まれた電子手帳に保存されていた個人データは、当該窃盗犯又はその後当該デバイスを入手する他のあらゆる人物にとって容易にアクセス可能であった。

94. This data breach concerns the confidentiality of the data stored on the stolen device.
これは、盗まれたデバイス内に保存されているデータの機密性に関わるデータ侵害である。

95. The notebook containing the personal data was vulnerable in this case because it did not possess any password protection or encryption. The lack of basic security measures enhances the risk level for the affected data subjects. Furthermore, the identification of

the concerned data subjects is also problematic, which also increases the severity of the breach. The considerable number of concerned individuals increases the risk, nevertheless, no special categories of personal data were concerned in the data breach.
この事例において、個人データが入った電子手帳は、パスワード保護又は暗号化が一切設定されていなかったため、脆弱であった。基本的な安全管理措置の欠如により、影響を受けたデータ主体に対するリスクレベルが高まる。さらに、関係するデータ主体の特定もまた問題であり、このことによっても侵害の深刻度は高まる。関係する個人の数の多さもリスクを高めるが、特別な種類の個人データは当該データ侵害に関わっていなかった。

96. During the risk assessment[29] the controller should take into consideration the potential consequences and adverse effects of the confidentiality breach. As a result of the breach the concerned data subjects may suffer identity fraud relying on the data available on the stolen device, so risk is considered to be high.
管理者は、リスク評価において [29]、機密性の侵害により生じる可能性のある結果及び悪影響について考慮しなければならない。侵害の結果、盗まれたデバイスに入っている利用可能なデータを使用し、関係するデータ主体が ID 詐欺の被害を受けうるため、リスクは高いとみなされる。

5.2.2 CASE No. 11 – Mitigation and obligations
5.2.2 事例 No.11—リスク低減措置及び義務

97. Turning on device encryption and the use of strong password protection of the stored database could have prevented the data breach to result in a risk to the rights and freedoms of the data subjects.
デバイスの暗号化を有効にし、保存されたデータベースに強力なパスワード保護を使用することにより、データ主体の権利及び自由に対するリスクをもたらすデータ侵害を防ぐことができた可能性がある。

98. Due to these circumstances the notification of the SA is required, the notification of the concerned data subjects is also necessary.
これらの状況から、SA に対する通知が要求され、また関係するデータ主体に対する通知も必須である。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

5.3 CASE No. 12: Stolen paper files with sensitive data
5.3 事例 No.12：センシティブデータの入った紙ファイルの盗難

A paper log book was stolen from a drug addiction rehab facility. The book contained basic identity and health data of the patients admitted to the rehab facility. The data was only stored on paper and no backup was available to the doctors treating the patients. The book was not stored in a locked drawer or a room, the data controller had neither an access control regime nor any other safeguarding measure for the paper

[29] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

documentation.
ある薬物依存症回復施設から紙の記録簿が盗まれた。当該記録簿には施設に入所している患者の基本的な身元情報及び健康に関するデータが記載されていた。データは紙でのみ保存されており、患者を治療する医師が使用できるバックアップは存在しなかった。当該記録簿は施錠された引出し又は部屋に保管されておらず、データ管理者は、当該紙の文書について、アクセス管理体制の他、いかなる保護措置も講じていなかった。

5.3.1 CASE No. 12 – Prior measures and risk assessment
5.3.1 事例 No.12—事前対策及びリスク評価

99. No prior safety measures were taken by the data controller, hence the personal data stored in this book was easily accessible for the person who found it. Moreover, the nature of the personal data stored in the book makes the lack of backup data a very serious risk factor.
データ管理者が事前の安全管理措置を講じていなかったため、当該記録簿に保存されていた個人データはこれを発見した人物にとって容易にアクセス可能であった。さらに、記録簿に保存されていた個人データの性質から、バックアップデータがないことは、非常に深刻なリスク要素となる。

100. This case serves as an example for a high-risk data breach. Due to the failure of appropriate safety precautions, sensitive health data pursuant to Article 9 (1) GDPR was lost. Since in this case a special category of personal data was concerned, the potential risks to the concerned data subjects was increased, which should be also taken into consideration by the controller assessing the risk[30].
この事例は、リスクの高いデータ侵害の一例となる。事前に適切な安全管理措置を講じていなかったことにより、GDPR 第 9 条第 1 項にいうセンシティブな健康に関するデータが失われた。この事例には特別な種類の個人データが関係していることから、関係するデータ主体に対し生ずる可能性のあるリスクが高くなる。管理者はリスク評価の際、このことも考慮に入れなければならない[30]。

101. This breach concerns the confidentiality, availability and integrity of the concerned personal data. As a result of the breach, medical secrecy is broken and unauthorized third parties may gain access to the patients' private medical information, what may have severe impact on the patient's personal life. The availability breach may also disturb the continuity of the patients' treatment. Since the modification/deletion of parts of the book's content may not be excluded, the integrity of the personal data is also compromised.
この侵害は、関係する個人データの機密性、可用性及び完全性に関わる。侵害の結果、医療上の秘密が損なわれ、無権限の第三者が患者の個人的な医療情報へアクセスしうる。このことは患者の私生活に深刻な影響を与えうるものである。可用性の侵害も、患者の治療の継続性を妨げうる。記録簿の記載内容の一部の変更／消去も除外できないため、個人データの完全性も損なわれる。

5.3.2 CASE No. 12 – Mitigation and obligations
5.3.2 事例 No.12—リスク低減措置及び義務

102. During the assessment of the safeguarding measures the type of the supporting asset should be considered as well. Since the patient log book was a physical document, its safeguarding should have been organized differently than that of an electronic device. The pseudonymisation of the patients' names, the storage of the book in a safeguarded premises and in a locked drawer or a room, and proper access control with authentication

[30] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

when accessing it could have prevented the data breach.
保護措置の評価の際には、当該サポートアセットの種類についても考慮しなければならない。当該患者の記録簿は物理的文書であるため、電子デバイスのものとは異なる保護措置が講じられるべきであった。患者の氏名の仮名化、安全性が確保された場所でかつ施錠された引出し又は部屋での記録簿の保管、並びにアクセス認証による適正なアクセス管理により、当該データ侵害を防ぐことができた可能性がある。

103. The above described data breach may severely impact the concerned data subjects; hence the notification of the SA and communication of the breach to the concerned data subjects is mandatory.
上記のデータ侵害は、関係するデータ主体に深刻な影響をもたらしうるため、SA に対する通知及び関係するデータ主体に対する連絡は義務である。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

5.4 Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices
5.4 デバイスの紛失又は盗難の防止／影響低減のための組織的及び技術的な措置

104. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.
下記の措置を組合せ、ケース毎の固有の特徴に応じて適用することで、同様の侵害の発生の可能性を低下させることに役立つであろう。

105. Advisable measures:
望ましい措置

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下記の措置のリストは、これ以外の措置を排除するものでも全てを網羅するものでもない。むしろ防止案及び考えられる解決策の提供を目的とするものである。取扱活動はそれぞれ異なるため、管理者は状況に応じて最適な措置を決定しなければならない。）

- Turn on device's encryption (such as Bitlocker, Veracrypt or DM-Crypt).
デバイスの暗号化を有効にする（Bitlocker、Veracrypt 又は DM-Crypt 等）。
- Use passcode/password on all devices. Encrypt all mobile electronic devices in a way that requires the input of a complex password for decryption.
全てのデバイスにパスコード／パスワードを設定する。全ての携帯型電子機器を、復号時に複雑なパスワードの入力が求められる方法で暗号化する。
- Use multi-factor authentication.
多要素認証を使用する。
- Turn on the functionalities of highly mobile devices that allow them to be located

in case of loss or misplacement.
紛失又は置忘れに備えて、持ち運びしやすいデバイスの位置を特定できるような機能を有効にする。

- Use MDM (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices.
  MDM（モバイルデバイス管理）ソフトウェア／アプリ及び位置特定機能を使用する。防眩フィルターを使用する。未使用のデバイスは全て閉じておく。
- If possible and appropriate to the data processing in question, save personal data not on a mobile device, but on a central back-end server.
  問題となるデータ取扱いについて、可能かつ適切な場合、個人データを携帯型機器ではなく中央管理のバックエンドサーバーに保存する。
- If the workstation is connected to the corporate LAN, do an automatic backup from the work folders provided it is unavoidable that personal data is stored there
  個人データをワークフォルダに保存することが避けられない場合、当該ワークステーションが企業 LAN に接続されているならば、ワークフォルダから自動バックアップを取る。
- Use a secure VPN (e.g. which requires a separate second factor authentication key for the establishment of a secure connection) to connect mobile devices to back-end servers.
  携帯型機器をバックエンドのサーバーに接続する際、（例えば、安全な接続の確立のために第 2 要素の認証鍵を別途要求するような）安全な VPN 接続を使用する。
- Provide physical locks to employees in order to enable them to physically secure mobile devices they use while they remain unattended.
  従業員が自身の使用する携帯型機器を使わない間、自身で機器を物理的に保護できるよう、従業員に物理的な鍵を提供する。
- Proper regulation of device usage outside the company.
  社外でのデバイスの使用に関する適正な規則。
- Proper regulation of device usage inside the company.
  社内でのデバイスの使用に関する適正な規則。
- Use MDM (Mobile Devices Management) software/app and enable the remote wipe function.
  MDM（モバイルデバイス管理）ソフトウェア／アプリを使用し、またリモートワイプ機能を有効にする。
- Use centralised device management with minimum rights for the end users to install software.
  端末のユーザーがソフトウェアをインストールすることについて、最低限の権利付与による一元化したデバイス管理を使用する。
- Install physical access controls.
  物理的なアクセス管理を導入する。
- Avoid storing sensitive information in mobile devices or hard drives. If there is need to access the company’s internal system, secure channels should be used such as previously stated.
  携帯型機器又はハードドライブにセンシティブな情報を保存しないようにする。会社の内部システムにアクセスする必要がある場合は、上記のような安全なチャンネルを使用する。

6 MISPOSTAL
6 誤郵送・誤送信

106. The risk source is an internal human error in this case as well, but here no malicious action led to the breach. It is the result of inattentiveness. Little can be undertaken by the controller after it happened, so prevention is even more important in these cases than in other breach types.
このケースのリスク源も、内部の人間によるヒューマンエラーであるが、ここでは悪意の行為により侵害が導かれるのではない。侵害は、不注意の結果である。当該侵害の発生後に管理者ができることはほとんどないため、この事例では他の種類の侵害に比べ、防止がより一層重要となる。

6.1 CASE No. 13: Postal mail mistake
6.1 事例 No.13：誤郵送

Two orders for shoes were packed by a retail company. Due to human error two packing bills were mixed up with the result that both products and the relevant packing bills were sent to the wrong person. This means that the two customers got each other's orders, including the packing bills containing the personal data. After becoming aware of the breach the data controller recalled the orders and sent them to the right recipients.
ある小売企業が 2 件の靴の注文を梱包した。ヒューマンエラーにより 2 件の梱包伝票が混同され、その結果両方の商品及び関連する梱包伝票がそれぞれ間違った注文主に送付された。このことは、2 人の顧客はそれぞれ、個人データが記載された梱包伝票を含む、他方の荷物を受領したことを意味する。侵害に気づいた後、データ管理者はこれらの注文の品を回収し、正しい受領者に送付した。

6.1.1 CASE No. 13 - Prior measures and risk assessment
6.1.1 事例 No.13—事前対策及びリスク評価

107. The bills contained the personal data required for a successful delivery (name, address, plus the item purchased and its price). It is important to identify how the human error could have happened in the first place, and if in any way, it could have been prevented. In the particular case describe the risk is low, since no special categories of personal data or other data whose abuse might lead to substantial negative effects were involved, the breach is not a result of a systemic error on the controller's part and only two individuals are concerned. No negative effect on the individuals could be identified.
伝票には納品の成功のために必要な個人データ（氏名、住所に加え、購入商品名とその価格）が記載されていた。当該ヒューマンエラーがそもそもどのようにして生じ得たのか、また、何らかの方法で防止することが可能であったかを特定することが重要である。この特定の事例では、特別な種類の個人データ又はその悪用により深刻な悪影響が生じるおそれのあるその他のデータが含まれていないこと、侵害が管理者側の機械システム上のエラーによるものではないこと、及び関与しているのが 2 人の個人のみであることから、リスクは低いことを表している。当該 2 名の個人に対する悪影響は認められないであろう。

6.1.2 CASE No. 13 – Mitigation and obligations
6.1.2 事例 No.13—リスク低減措置及び義務

108. The controller should provide for a free return of the items and the accompanying bills, and it also should request the wrong recipients to destroy / delete all eventual copies of the bills containing the other person's personal data.

管理者は、商品及び添付の伝票について無料返送を提供しなければならない。また管理者は、間違った受領者に対し、他方の人物の個人データを記載した当該伝票の全ての最終的な複製物を破棄／消去するよう要請しなければならない。

109. Even if the breach itself does not pose a high risk to rights and freedoms of the affected individuals, and thus communication to the data subjects is not mandated by Article 34 GDPR, communication of the breach to them cannot be avoided, as their cooperation is needed to mitigate the risk.
当該侵害自体は、影響を受けた個人の権利及び自由に対し高いリスクをもたらすものではなく、従ってデータ主体に対する連絡が GDPR 第 34 条により義務づけられていないが、リスク低減のためにデータ主体の協力が必要となるため、データ主体への侵害の連絡は避けられない。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

6.2 CASE No. 14: Highly confidential personal data sent by mail by mistake
6.2 事例 No.14：秘匿性の高い個人データのメールによる誤送信

The employment department of a public administration office sent an e-mail message – about upcoming trainings - to the individuals registered in its system as jobseekers. By mistake, a document containing all these jobseekers' personal data (name, e-mail address, postal address, social security number) was attached to this e-mail. The number of affected individuals is more than 60000. Subsequently the office contacted all the recipients and asked them to delete the previous message and not to use the information contained in it.
ある行政機関の雇用担当部署が、求職者としてシステムに登録されている個人に対し、開催予定の訓練について、電子メールを送付した。誤って、当該求職者全員の個人データ（氏名、電子メールアドレス、住所、社会保障番号）が記載された文書を当該電子メールに添付していた。影響を受けた個人の数は 6 万人以上である。その後、当該担当部署は、電子メールの受信者全員に連絡し、先に送付したメッセージを消去するよう、また当該メッセージに含まれている情報を使用しないよう要請した。

6.2.1 CASE No. 14 - Prior measures and risk assessment
6.2.1 事例 No.14—事前対策及びリスク評価

110. Stricter rules should have been implemented for sending such messages. The introduction of additional control mechanisms need to be considered.
このようなメッセージの送信について、より厳格なルールを実装しておくべきであった。追加的な管理の仕組みの導入を検討する必要がある。

111. The number of affected individuals is considerable, and the involvement of their social security number, along with other, more basic personal data, further increases the risk, which can be identified as high[31]. The eventual distribution of the data by any of the recipients cannot be contained by the controller.

[31] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

影響を受けた個人の数が甚大であること、また他のより基本的な個人データと伴に社会保障番号が含まれていることが更にリスクを上げ、結果、リスクは高いと特定される可能性がある [31]。管理者は、受領者のいずれかによる今後のデータの拡散を阻止することはできない。

6.2.2 CASE No. 14 – Mitigation and obligations
6.2.2 事例 No.14—リスク低減措置及び義務

112. As mentioned earlier, the means to effectively mitigate the risks of a similar breach, are limited. Though the controller asked for the deletion of the message, it cannot force the recipients to do so, and as a consequence, nor can it be certain that they comply with the request.
前述のとおり、このような侵害によるリスクを効果的に低減する方法は限られている。管理者は受領者に対しメッセージの削除を求めたが、管理者は受信者らにそうするよう強制することはできず、また結果として、受領者が要請に従うか確信することもできない。

113. The execution of all three below indicated actions should be self-evident in a case like this.
以下に示す 3 つ全ての措置を実施することは、このようなケースにおいては自明である。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

6.3 CASE No. 15: Personal data sent by mail by mistake
6.3 事例 No.15：個人データのメールによる誤送信

A list of participants on a course in Legal English which takes place in a hotel for 5 days is by mistake sent to 15 former participants of the course instead of the hotel. The list contains names, e-mail addresses and food preferences of the 15 participants. Only two participants have filled in their food preferences, stating that they are lactose intolerant. None of the participants have a protected identity. The controller discovers the mistake immediately after sending the list and informs the recipients of the mistake and asks them to delete the list.
あるホテルで 5 日間にわたり開催される法律英語のコースの参加者リストが、誤って、ホテルにではなくコースの過去の参加者 15 名に送付される。リストには当該過去の参加者 15 名の氏名、電子メールアドレス及び食の嗜好が記載されている。2 名の参加者のみが食の嗜好欄に乳糖不耐症である旨記入している。いずれの参加者についても、要保護の個人情報はない。管理者はリストの送信直後に誤送信に気づき、受領者に対し誤送信の旨を通知し、リストを消去するよう要請する。

6.3.1 CASE No. 15 - Prior measures and risk assessment
6.3.1 事例 No.15—事前対策及びリスク評価

114. Strict rules should have been implemented for sending of messages containing personal data. The introduction of additional control mechanisms need to be considered.
個人データを含むメッセージの送信について、厳格なルールを実装しておくべきであった。追加的な管理の仕組みの導入を検討する必要がある。

115. The risks deriving from the nature, the sensitivity, the volume and the context of the personal data are low. The personal data includes sensitive data on food preferences of two of the participants. Even if the information that someone is lactose intolerant is health data, the risk that this data will be used in a detrimental way should be considered relatively low. While in the case of data concerning health it is usually assumed that the breach is likely to result in a high risk for the data subject[32], at the same time in this particular case no risk can be identified that the breach will lead to physical, material or non-material damages of the data subject due to the unauthorised disclosure of lactose intolerance information. Contrary to some other food preferences, lactose intolerance can normally not be linked to any religious or philosophical beliefs. The quantity of the breached data and the number of affected data subjects is very low as well.
個人データの性質、機微性、量及び過程から生ずるリスクは低い。個人データには参加者 2 名の食の嗜好についてのセンシティブデータが含まれている。ある人物が乳糖不耐症であるという情報は健康に関するデータではあるものの、当該データが悪影響をもたらす形で利用されるリスクは比較的低いとみなされるであろう。健康に関するデータの場合、その侵害は通常、データ主体に高いリスクをもたらすおそれがあると想定されるが [32]、同時にこの特定の事例では、乳糖不耐症であるという情報の無権限の開示により、当該侵害がデータ主体の物的な損失、財産的な損失又は非財産的な損失につながるといったリスクを特定することができない。他の食の嗜好と異なり、乳糖不耐症は通常、いかなる宗教的又は思想的な信念とも関連付けられる可能性はない。侵害を受けたデータの量及びデータ主体の数も非常に少ない。

6.3.2 CASE No. 15 – Mitigation and obligations
6.3.2 事例 No.15—リスク低減措置及び義務

116. In summary, it can be stated that the breach had no significant effect on the data subjects. The fact that the controller immediately contacted the recipients after becoming aware of the mistake can be considered as a mitigating factor.
概して、当該侵害はデータ主体に重大な影響を及ぼさなかったと言える。管理者が当該誤りに気づいた直後に受領者に連絡したという事実は、リスク低減要素とみなすことができる。

117. If an email is sent to an incorrect/unauthorised recipient, it is recommended that the data controller should Bcc a follow up email to the unintended recipients apologising, instructing that the offending email should be deleted, and advising recipients that they do not have the right to further use the email addresses identified to them.
誤った／無権限の相手に電子メールが送信される場合、データ管理者は意図されてない受信者に対し、謝罪し、問題のある電子メールの消去を指示し、知り得た電子メールアドレスを追加的に使用する権限がない旨を助言すべく、フォローアップの電子メールを BCC で送るよう勧告する。

118. Due to these facts this data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the SA or the concerned data subjects was necessary. However, this data breach must also be documented in accordance with Article 33(5).
これらの事実から、当該データ侵害は、データ主体の権利及び自由に対するリスクをもたらすおそれがなく、従って、該当の SA 又は関係するデータ主体に対する

[32] See Guidelines WP 250, p. 23.
ガイドライン WP250、P23 参照。

侵害通知は必要なかった。しなしながら、当該データ侵害においても GDPR 第 33 条第 5 項に基づく文書化は必須である。

Actions necessary based on the identified risks 特定されたリスクに基づき必要となる措置		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	X	X

6.4 CASE No. 16: Postal mail mistake
6.4 事例 No.16：誤郵送

An insurance group offers car insurances. To do this, it sends out regularly adjusted contribution policies by postal mail. In addition to the name and address of the policyholder, the letter contains the vehicle registration number without masked digits, the insurance rates of the current and next insurance year, the approximate annual mileage and the policyholder's date of birth. Health data according to Article 9 GDPR, payment data (bank details), economic and financial data are not included.
ある保険グループが自動車保険を提供している。このため、保険契約証券の更新版を定期的に郵送している。当該郵送書類には、加入者の氏名及び住所に加え、数字が隠されていない車両登録番号、当年度及び翌年度の保険料率、年間走行距離の概算値並びに加入者の生年月日が記載されている。GDPR 第 9 条にいう健康に関するデータ、支払データ（銀行の詳細情報）、経済性のデータ及び財務データは含まれていない。

Letters are packed by automated enveloping machines. Due to a mechanical error, two letters for different policyholders are inserted into one envelope and sent to one policyholder by letter post. The policyholder opens the letter at home and takes a look at his correctly delivered letter as well as at the incorrectly delivered letter from another policyholder.
書類は自動封入機で封入されている。機械上のエラーにより、異なる加入者 2 名分の書類が 1 つの封筒に封入され、1 名の加入者に郵送される。これを受領した加入者は郵便物を自宅で開封し、正しく配達された自身の書類に加え、誤って配達された別の加入者宛の書類も一見する。

6.4.1 CASE No. 16 – Prior measures and risk assessment
6.4.1 事例 No.16—事前対策及びリスク評価

119. The incorrectly delivered letter contains the name, address, date of birth, unmasked vehicle registration number and the classification of the insurance rate of the current and the next year. The effects on the affected person are to be regarded as medium, since information not publicly available such as the date of birth or unmasked vehicle registration numbers, and details about the increment in insurance rates are disclosed to the unauthorized recipient. The probability of misuse of this data is assessed to be between low and medium. However, while many recipients will probably dispose of the wrongly received letter in the garbage, in individual cases it cannot be completely ruled out that the letter will be posted in social networks or that the policyholder will be contacted.
誤って送付された書類には、加入者の氏名、住所、生年月日、隠されていない車両登録番号及び当年度と翌年度の保険料率の等級が記載されている。生年月日又は車両登録番号、及び保険料率の上昇に関する情報といった非公開の情報が無権

限の受領者に開示されることから、被害を受けた個人への影響は中程度とみなされるであろう。当該データが悪用される可能性は、低から中程度であると評価される。しかしながら、多くの受領者はおそらく誤って受領した文書を破棄するであろうが、個々のケースにおいて、当該書類が SNS 上に投稿される、又は加入者が連絡を受けるといったことを完全には除外できない。

6.4.2 CASE No. 16 – Mitigation and obligations
6.4.2 事例 No.16—リスク低減措置及び義務

120. The controller should have the original document returned at its own expense. The wrong recipient should also be informed that he/she may not misuse the information read.
管理者は自ら費用負担をして、当該書類原本を返送させなければならない。また間違った受取人に対し、読んだ情報を悪用してはならない旨を通知しなければならない。

121. It will probably never be possible to completely prevent a postal delivery error in a mass mailing using fully automated machines. However, in the event of an increased frequency, it is necessary to check whether the enveloping machines are set and maintained correctly enough, or if some other systemic issue leads to such a breach.
全自動の機械による大量郵送において、誤郵送を完全に防止することはおそらく不可能である。しかし、頻度が増える場合は、封入機が十分正確に設定され維持されているか、又はそのような侵害につながる他の何らかのシステム上の問題がないか確認する必要がある。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	X

6.5 Organizational and technical measures for preventing / mitigating the impacts of mispostal
6.5 誤郵送・誤送信の防止／影響低減のための組織的及び技術的な措置

122. A combination of the below mentioned measures – applied depending on the unique features of the case – should help to lower the chance of a similar breach reoccurring.
下記の措置を組合せ、ケース毎の固有の特徴に応じて適用することで、同様の侵害の発生の可能性を低下させることに役立つであろう。

123. Advisable measures:
望ましい措置

(*The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.*)
（下記の措置のリストは、これ以外の措置を排除するものでも全てを網羅するものでもない。むしろ防止案及び考えられる解決策の提供を目的とするものである。取扱活動はそれぞれ異なるため、管理者は状況に応じて最適な措置を決定しなければならない。）

- Setting exact standards – with no room for interpretation – for sending letters / e-

mails.
郵便物の送付／電子メールの送信について、解釈の余地のない、明確な基準を設定する。

- Adequate training for personnel on how to send letters / e-mails.
  郵便物の送付／電子メールの送信方法について、職員に適切な訓練を実施する。
- When sending e-mails to multiple recipients, they are listed in the 'bcc' field by default.
  複数の受信者に電子メールを送信する場合、デフォルト設定で『BCC』フィールドに宛先を列記する。
- Extra confirmation is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
  複数の受信者に電子メールを送信し、『BCC』フィールドに宛先が列記されていない場合は、追加の確認を要求する。
- Application of the four-eyes principle.
  ４つ目原則の適用。
- Automatic addressing instead of manual, with data extracted from an available and up-to-date database; the automatic addressing system should be regularly reviewed to check for hidden errors and incorrect settings.
  宛名を手動ではなく、利用可能で最新のデータベースから抽出したデータを使用して自動で入力する。また、自動宛名入力のシステムを定期的に見直し、隠れたエラー及び間違った設定の有無を確認する。
- Application of message delay (e.g. the message can be deleted / edited within a certain time period after clicking the press button).
  メッセージ遅延送信機能（例えば、送信ボタンをクリックした後一定時間内はメッセージの消去／編集が可能）の適用。
- Disabling autocomplete when typing in e-mail addresses.
  電子メールアドレスの入力時のオートコンプリート機能を無効にする。
- Awareness sessions on most common mistakes leading to a personal data breach.
  個人データ侵害につながる、最も一般的な誤りについて意識向上のためのセッションを設ける。
- Training sessions and manuals on how to handle incidents leading to a personal data breach and who to inform (involve DPO).
  個人データ侵害につながるインシデントの対応方法及び報告先（データ保護オフィサーを含む）に関し、訓練のためのセッションを設け、マニュアルを策定する。

7 OTHER CASES – SOCIAL ENGINEERING
7 その他の事例―ソーシャルエンジニアリング攻撃

7.1 CASE No. 17: Identity theft
7.1 事例 No.17：ID 盗取

The contact centre of a telecommunication company receives a telephone call from someone that poses as a client. The supposed client demands the company to change the email address to which the billing information should be sent from there on. The worker of the contact centre validates the client's identity by asking for certain personal data, as defined by the procedures of the company. The caller correctly indicates the requested client's fiscal number and postal address (because he had

access to these elements). After the validation, the operator makes the requested change and, from there on, the billing information is sent to the new email address. The procedure does not foresee any notification to the former email contact. The following month the legitimate client contacts the company, inquiring why he is not receiving billing to his email address, and denies any call from him demanding the change of the email contact. Later, the company realizes that the information has been sent to an illegitimate user and reverts the change.

ある電気通信会社のコンタクトセンターが、顧客を装った人物からの電話を受ける。当該顧客と思われる人物は会社に対し、今後の請求情報の送付先である電子メールアドレスの変更を求める。コンタクトセンターの職員は会社が定める手順に従い、一定の個人データに関する質問をし、当該顧客の本人確認を行う。電話の主は、その要請された顧客の財務番号及び住所を正確に答える（当該情報にアクセスしていたからである）。本人確認後、オペレーターは要求された変更を行い、以降、請求情報は新しい電子メールアドレスに送信されることになる。当該手順では、変更前の電子メールの連絡先への通知は一切行われない。翌月、正当な顧客が当該会社に連絡し、自身の電子メールアドレス宛に請求情報が届いていない理由を尋ね、連絡先の電子メールの変更を要求する一切の電話について否定する。その後、会社は正当な顧客ではない人物に情報が送信されていることに気付き、電子メールアドレスの変更を元に戻す。

7.1.1 CASE No. 17 – Risk assessment, mitigation and obligations
7.1.1 事例 No.17—リスク評価、リスク低減措置及び義務

124. This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk[33], as billing data can give information about the data subject's private life (e.g. habits, contacts) and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organization or exploit further authentication measures in other organisations. Considering these risks, the "appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication.

この事例は事前の対策の重要性を示す一例である。請求情報からデータ主体の私生活（習慣、連絡先、等）に関する情報が分かる可能性があり、物理的な損害（ストーキング、身体の完全性に対する危険等）に繋がる可能性があることから、当該侵害は、リスクの側面からみると、高いリスクレベルを示している [33]。この攻撃中に取得された個人データはまた、同組織内でアカウントを乗っ取るため、又は他の組織で更なる認証手段を割り出すために使用される可能性もある。これらのリスクを考慮し、「適切な」認証方法というものは、認証の結果処理することが可能となる個人データの種類に応じて、高い基準を満たすものでなければならない。

125. As a result, both a notification to the SA and a communication to the data subject are needed from the controller.

結果として、管理者は SA に対する通知及びデータ主体に対する連絡の両方が必要となる。

126. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be

[33] For guidance on "likely to result in high risk" processing operations, see footnote 10 above.
「高いリスクをもたらすおそれのある」取扱業務に関するガイダンスは、前掲、脚注 10 を参照。

the intended user by the use of publicly available information and information that they otherwise had access to.
この事件を踏まえ、事前の顧客の確認プロセスは、明らかに改善されなければならない。認証のために使用された方法は不十分であった。当該悪意のある者は、公開されている情報及び別途アクセスした情報を用いて、意図されたユーザーになりすますことができた。

127. The use of this type of static knowledge-based authentication (where the answer does not change, and where the information is not "secret" such as would be the case with a password) is not recommended.
この種の静的な知識ベースの認証（答えが変わらないとき、またパスワードの場合にあるようにその情報が「秘密」ではないとき）の使用は推奨されない。

128. Instead, the organization should use a form of authentication which would result in a high degree of confidence that the authenticated user is the intended person, and not anyone else. The introduction of an out-of-band multi-factor authentication method would solve the problem, e.g. to verify the change demand, by sending a confirmation request to the former contact; or adding extra questions and requiring information only visible on the previous bills. It is the controller's responsibility to decide which measures to introduce, as it knows the details and requirements of its internal operation the best.
代わりに、当該組織は、認証された人物が意図されている人物であり、他の何者でもないということを高い信頼度でもたらすような認証の形式を使用しなければならない。多要素を使用した帯域外認証を行う方法、例えば、当該変更の要求を確認するために変更前の連絡先に確認要請を送信するという方法、又は追加的な質問をし、過去の請求書からのみ確認可能な情報を要求するといった方法を導入することにより、この問題は解決されるであろう。管理者がその内部業務の詳細及び要件を最も理解しているため、どの方法を導入するかを決定するのは管理者の責務である。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔

7.2 CASE No. 18: Email exfiltration
7.2 事例 No.18：電子メールの窃取

A hypermarket chain detected, 3 months after its configuration, that some email accounts had been altered and rules created so that every email containing certain expressions (e.g. "invoice", "payment", "bank wiring", "credit card authentication", "bank account details") would be moved to an unused folder and also forwarded to an external email address. Also, by that time, a social engineering attack had already been performed, i.e., the attacker, posing as a supplier, had had that supplier bank account details altered into his own. Finally, by that time, several fake invoices had been sent that included the new bank account detail. The monitoring system of the email platform ended up giving an alert regarding the folders. The company was unable to detect how the attacker was able to gain access to the email accounts to begin with, but it supposed that an infected email was to blame for giving access to the group of

users in charge of the payments.
ある大型スーパーマーケットチェーンは、一部の電子メールアカウントが変更されていたこと、また一定の表現（「請求書」「支払」「銀行送金」「クレジットカード認証」「銀行口座情報」等）を含む全ての電子メールがある使用されていないフォルダーに移動され、外部の電子メールアドレス宛に転送されるようにルールが設定されていたことを、当該設定の 3 カ月後に検出した。またその時点までに、ソーシャルエンジニアリング攻撃が既に実行されていた。具体的には、攻撃者がある仕入先を装い、当該仕入先の銀行口座情報を攻撃者のものに変更していた。最終的にはその時点までに、当該新規の銀行口座情報が記載された複数の偽の請求書が送付されていた。結局、当該電子メールのプラットフォームの監視システムがフォルダーに関する警告を発信した。会社は、第一に、攻撃者がどのようにして電子メールアカウントにアクセスできたか特定できなかったが、ある感染した電子メールが支払担当者のユーザーグループにアクセスを与えたことが原因ではないかと推測した。

Due to the keyword-based forwarding of emails, the attacker received information on 99 employees: name and wage of a particular month regarding 89 data subjects; name, civil status, number of children, wage, work hours and remainder information on the salary receipt of 10 employees whose contracts were ended. The controller only notified the 10 employees belonging to the latter group.
電子メールがキーワードベースで転送されたことで、攻撃者は、従業員 99 人に関する情報、具体的には、89 人分のデータ主体の氏名とある特定の月の賃金、並びに契約が終了していた従業員 10 人分の氏名、婚姻状況、子どもの人数、賃金、勤務時間及びその他の給与受領に関する情報を取得した。管理者は、契約が終了していたグループに属する従業員 10 人に対してのみ侵害を通知した。

7.2.1 CASE No. 18 - Risk assessment, mitigation and obligations
7.2.1 事例 No.18—リスク評価、リスク低減措置及び義務

129. Even if the attacker was probably not aiming at collecting personal data, since the breach could lead to both material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud), or the data could be used to facilitate other attacks (e.g. phishing), the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Therefore the breach should be communicated to all 99 employees and not only to the 10 employees whose salary information was leaked.
攻撃者の目的が個人データの収集ではないと予想される場合でも、当該侵害が財産的な損失（金銭的損失等）及び非財産的な損失（ID 盗取又は ID 詐欺等）の両方につながる可能性があること、又は当該データが他の攻撃（フィッシング等）をするために使用される可能性があることから、当該個人データ侵害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。そのため、その給与受領に関する情報が漏洩した 10 人の従業員だけでなく、99 人の従業員全員に当該侵害を連絡しなければならない。

130. After becoming aware of the breach, the controller forced a password change for the compromised accounts, blocked sending emails to the attacker's email account, notified the service provider of the email used by the attacker regarding his or her actions, removed the rules set by the attacker and refined the alerts of the monitoring system in order to give an alert as soon as an automatic rule is created. Alternatively, the controller could remove the right for users to set forwarding rules, needing the IT service team to do it only

on request or it could introduce a policy that users should check and report on the rules set on their accounts once per week or more often, in areas handling financial data.
管理者は、侵害に気づいた後、不正アクセスのあったアカウントのパスワードを強制的に変更し、攻撃者の電子メールアカウントへの電子メール送信をブロックし、攻撃者が使用した電子メールのサービスプロバイダに対しその行為について通知し、攻撃者が設定したルールを削除し、自動設定ルールが作成された場合直ちに警告を出すよう監視システムのアラートを改善した。これに代わる措置として、財務データを取扱う部署においては、管理者がユーザーから転送ルールの設定の権限を取り除き、転送ルールの設定は要請があった場合にのみ IT サービスチームが行うよう求める、又は、自身のアカウントについて設定されているルールについてユーザーが週に一回以上確認し報告するという方針を管理者が導入することができよう。

131. The fact that a breach could happen and go undetected for so long and the fact that, in a longer time, social engineering could have been used for altering more data, highlighted significant problems in the controller's IT security system. These should be addressed without delay, like emphasizing automation reviews and change controls, incident detection and response measures. Controllers handling sensitive data, financial information, etc. have a larger responsibility in terms of providing adequate data security.
侵害が発生し長期間検知されない可能性があるという事実、及び、より長い期間にソーシャルエンジニアリング攻撃がより多くのデータの改変のために使用されていた可能性があるという事実は、管理者の IT のセキュリティシステムに重大な問題点があることを強調した。これらの問題点は、自動設定の再確認及び変更の管理、インシデント検知、並びに対応措置を強化するといったように、遅滞なく対処されなければならない。センシティブデータ、財務情報等を扱う管理者は、適切なデータの安全性を提供することに関して、より大きな責任を負う。

Actions necessary based on the identified risks **特定されたリスクに基づき必要となる措置**		
Internal documentation 内部文書化	Notification to SA SA に対する通知	Communication to data subjects データ主体に対する連絡
✔	✔	✔