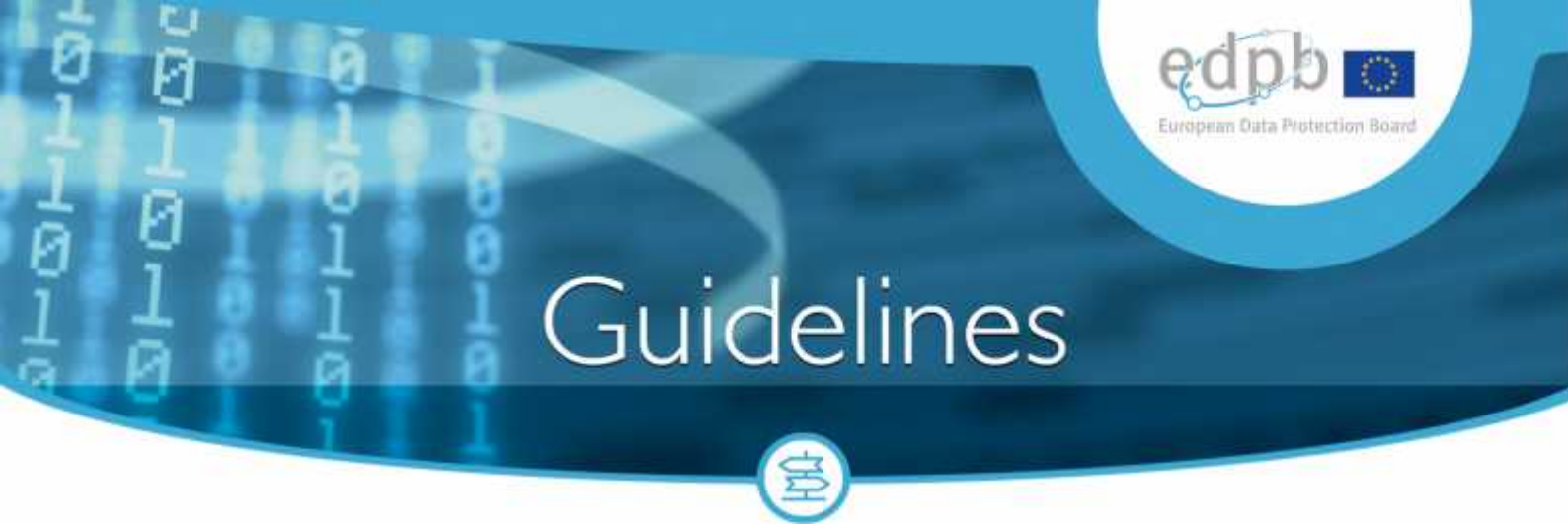

Guidelines 01/2021

on Examples regarding Personal Data Breach Notification

Adopted on 14 December 2021

Version 2.0

Version history

Version 2.0	14 12 2021	Adoption of the Guidelines after public consultation
Version 1.0	14 01 2021	Adoption of the Guidelines for public consultation

Table of contents

THE EUROPEAN DATA PROTECTION BOARD

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"),

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],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

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],

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

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).

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 "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.

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.

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

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[2] COM(2020) 264 final, 24 June 2020.

[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.

accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

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:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.[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.

7. Accordingly, the GDPR requires the controller to:

- document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken[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];
- 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 persons[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

[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 .

[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.

[6] GDPR Article 33(5).

[7] GDPR Article 33(1).

[8] GDPR Article 34(1).

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].

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.

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

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

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.

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.

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.

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.

[9] GDPR Article 33(4).

2 RANSOMWARE

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.

2.1 CASE No. 01: Ransomware with proper backup and without exfiltration

> 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.

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.

2.1.1 CASE No. 01 - Prior measures and risk assessment

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.

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.

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.

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 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.

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).

2.1.2 CASE No. 01 – Mitigation and obligations

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.

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.

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

---

[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.

[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.

[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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

2.2 CASE No. 02: Ransomware without proper backup

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.

2.2.1 CASE No. 02 - Prior measures and risk assessment

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.

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.

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.

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

[13] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

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.

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.

31. The absence of a backup database can be considered a risk enhancing factor depending on the severity of consequences for the data subjects resulting from the lack of availability of the data.

2.2.2 CASE No. 02 – Mitigation and obligations

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.

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.

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.

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

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

[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.

2.3 CASE No. 03: Ransomware with backup and without exfiltration in a hospital

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.

2.3.1 CASE No. 03 - Prior measures and risk assessment

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].

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.

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.

2.3.2 CASE No. 03 – Mitigation and obligations

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 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.

[15] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

[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*".

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

2.4 CASE No. 04: Ransomware without backup and with exfiltration

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 by the attacker.

2.4.1 CASE No. 04 - Prior measures and risk assessment

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.

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].

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.

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.

[17] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

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).

2.4.2 CASE No. 04 – Mitigation and obligations

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).

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

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.

49. Advisable measures:

(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.)

- 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.
- 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.
- 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).
- Having / obtaining an appropriate, up-to-date, effective and integrated anti-malware software.

- 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).
- 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.
- 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.
- Forwarding or replication all logs to a central log server (possibly including the signing or cryptographic time-stamping of log entries).
- Strong encryption and multi factor authentication, in particular for administrative access to IT systems, appropriate key and password management.
- Vulnerability and penetration testing on a regular basis.
- 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.
- When assessing countermeasures – risk analysis should be reviewed, tested and updated.

3 DATA EXFILTRATION ATTACKS

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.

3.1 CASE No. 05: Exfiltration of job application data from a website

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.

3.1.1 CASE No. 05 - Prior measures and risk assessment

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).

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.

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].

3.1.2 CASE No. 05 – Mitigation and obligations

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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

[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.

[19] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

3.2 CASE No. 06: Exfiltration of hashed password from a website

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.

3.2.1 CASE No. 06 - Prior measures and risk assessment

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.

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.

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.

3.2.2 CASE No. 06 – Mitigation and obligations

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.

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.

61. The breach should be documented in accordance with Article 33 (5) but no notification or communication needed.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

[20] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

3.3 CASE No. 07: Credential stuffing attack on a banking website

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.

3.3.1 CASE No. 07 - Prior measures and risk assessment

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.

64. The breach concerns financial data beyond the identity and user ID information, making it particularly severe. The number of individuals affected is high.

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 run a spear phishing campaign directed at the bank customers.

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.

3.3.2 CASE No. 07 – Mitigation and obligations

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

[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.

[22] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

as adding two-factor authentication to the concerned website and moving up to a strong customer authentication.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

3.4 Organizational and technical measures for preventing / mitigating the impacts of hacker attacks

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.

70. Advisable measures:[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*.)

- 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.
- 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.
- Use of strong authentication methods like two-factor authentication and authentication servers, complemented by an up-to-date password policy.
- Secure development standards include the filtering of user input (using white listing as 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.
- Strong user privileges and access control management policy in place.
- Use of appropriate, up-to-date, effective and integrated firewall, intrusion detection and other perimeter defence systems.
- Systematic IT security audits and vulnerability assessments (penetration testing).
- Regular reviews and testing to ensure that backups can be used to restore any data whose integrity or availability was affected.
- No session ID in URL in plain text.

[23] For secure web application development see also: https://www.owasp.org/index.php/Main_Page .

4 INTERNAL HUMAN RISK SOURCE

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.

4.1 CASE No. 08: Exfiltration of business data by an employee

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

4.1.1 CASE No. 08 - Prior measures and risk assessment

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 employee 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.

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.

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].

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

[25] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

4.1.2 CASE No. 08 – Mitigation and obligations

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.

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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

4.2 CASE No. 09: Accidental transmission of data to a trusted third party

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.

4.2.1 CASE No. 09 – Prior measures and risk assessment

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.

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.

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.

4.2.2 CASE No. 09 – Mitigation and obligations

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.

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

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

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

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.

84. Advisable measures:

(*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.*)

- 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.
- Establishment of robust and effective data protection and privacy practices, procedures and systems[27].
- Evaluation of privacy practices, procedures and systems to ensure continued effectiveness[28].
- Making proper access control policies and forcing users to follow the rules.
- Implementing techniques to force user authentication when accessing sensitive personal data.
- Disabling the company related account of the user as soon as the person leaves the company.
- Checking unusual dataflow between the file server and employee workstations.
- 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.).
- 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).
- Disabling open cloud services.
- Forbidding and preventing access to known open mail services.
- Disabling print screen function in OS.
- Enforcing a clean desk policy.
- Automated locking all computers after a certain amount of time of inactivity.
- Use mechanisms (e.g. (wireless) token to log on/open locked accounts) for fast user switches in shared environments.
- Use of dedicated systems for managing personal data that apply appropriate access 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.

5 LOST OR STOLEN DEVICES AND PAPER DOCUMENTS

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.

[26] Section 2) subsection (i) of the Resolution to address the role of human error in personal data breaches.

[27] Section 2) subsection (ii) of the Resolution to address the role of human error in personal data breaches.

[28] Section 2) subsection (iii) of the Resolution to address the role of human error in personal data breaches.

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.

87. The scenarios bellow demonstrate how the above mentioned circumstances influence the likelihood and severity of the data breach.

5.1 CASE No. 10: Stolen material storing encrypted personal data

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.

5.1.1 CASE No. 10 - Prior measures and risk assessment

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).

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.

5.1.2 CASE No. 10 – Mitigation and obligations

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.

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.

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).

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

5.2 CASE No. 11: Stolen material storing non-encrypted personal data

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.

5.2.1 CASE No. 11 - Prior measures and risk assessment

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.

94. This data breach concerns the confidentiality of the data stored on the stolen device.

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.

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.

5.2.2 CASE No. 11 – Mitigation and obligations

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.

98. Due to these circumstances the notification of the SA is required, the notification of the concerned data subjects is also necessary.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

5.3 CASE No. 12: Stolen paper files with sensitive data

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 documentation.

[29] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

5.3.1 CASE No. 12 – Prior measures and risk assessment

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.

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].

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.

5.3.2 CASE No. 12 – Mitigation and obligations

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 when accessing it could have prevented the data breach.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

5.4 Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices

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.

105. Advisable measures:

(*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.*)

- Turn on device's encryption (such as Bitlocker, Veracrypt or DM-Crypt).
- Use passcode/password on all devices. Encrypt all mobile electronic devices in a way that requires the input of a complex password for decryption.
- Use multi-factor authentication.
- Turn on the functionalities of highly mobile devices that allow them to be located in case of loss or misplacement.

[30] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

- Use MDM (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices.
- 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.
- 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
- 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.
- Provide physical locks to employees in order to enable them to physically secure mobile devices they use while they remain unattended.
- Proper regulation of device usage outside the company.
- Proper regulation of device usage inside the company.
- Use MDM (Mobile Devices Management) software/app and enable the remote wipe function.
- Use centralised device management with minimum rights for the end users to install software.
- Install physical access controls.
- 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.

6 MISPOSTAL

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.

6.1 CASE No. 13: Postal mail mistake

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.

6.1.1 CASE No. 13 - Prior measures and risk assessment

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.

6.1.2 CASE No. 13 – Mitigation and obligations

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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

6.2 CASE No. 14: Highly confidential personal data sent by mail by mistake

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.

6.2.1 CASE No. 14 - Prior measures and risk assessment

110. Stricter rules should have been implemented for sending such messages. The introduction of additional control mechanisms need to be considered.

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.

6.2.2 CASE No. 14 – Mitigation and obligations

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.

113. The execution of all three below indicated actions should be self-evident in a case like this.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

6.3 CASE No. 15: Personal data sent by mail by mistake

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.

6.3.1 CASE No. 15 - Prior measures and risk assessment

114. Strict rules should have been implemented for sending of messages containing personal data. The introduction of additional control mechanisms need to be considered.

[31] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

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.

6.3.2 CASE No. 15 – Mitigation and obligations

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.

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.

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).

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

6.4 CASE No. 16: Postal mail mistake

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.

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.

6.4.1 CASE No. 16 - Prior measures and risk assessment

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

[32] See Guidelines WP 250, p. 23.

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.

6.4.2 CASE No. 16 – Mitigation and obligations

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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

6.5 Organizational and technical measures for preventing / mitigating the impacts of mispostal

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.

123. Advisable measures:

(*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.*)

- Setting exact standards – with no room for interpretation - for sending letters / e-mails.
- Adequate training for personnel on how to send letters / e-mails.
- When sending e-mails to multiple recipients, they are listed in the 'bcc' field by default.
- Extra confirmation is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
- Application of the four-eyes principle.
- 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.
- Application of message delay (e.g. the message can be deleted / edited within a certain time period after clicking the press button).
- Disabling autocomplete when typing in e-mail addresses.
- Awareness sessions on most common mistakes leading to a personal data breach.
- Training sessions and manuals on how to handle incidents leading to a personal data breach and who to inform (involve DPO).

7 OTHER CASES – SOCIAL ENGINEERING

7.1 CASE No. 17: Identity theft

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.

7.1.1 CASE No. 17 - Risk assessment, mitigation and obligations

124. This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk33, 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 organisation 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.

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

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 the intended user by the use of publicly available information and information that they otherwise had access to.

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.

128. Instead, the organisation 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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

[33] For guidance on "*likely to result in high risk*" processing operations, see footnote 10 above.

7.2 CASE No. 18: Email exfiltration

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.

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.

7.2.1 CASE No. 18 - Risk assessment, mitigation and obligations

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.

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.

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.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓