RESPONSE

TO THE PUBLIC CONSULTATION

"Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on January 14, 2021, Version 1.0."

01st March 2021

To the kind attention of

the European Data Protection Board

Rue Montoyer 30, B-1000 Brussels, Belgium

Who is dataTENET

dataTENET is an italian multi-disciplinary Team that includes Jurists, Data Privacy Lawyers, DPOs, IT Security Specialists, and Managers providing GDPR related services to public and private companies and entities.

We are scholars and enthusiasts of the thorniest issues related to the defense of fundamental rights and freedoms, the enhancement and freedom of circulation of personal data and the security of the related processing of personal data in the global society in rapid digital transformation.

dataTENET appreciates the opportunity to present their comments to the recently published EDPB Guidelines 01/2021 opened to the public consultation.

dataTENET team contributors to the Guidelines' analysis

BARBARA CALDERINI Jurist - Business Owner - Compliance Manager

GIANMARCO CENCI Lawyer - Data Protection Officer

SALVATORE COPPOLA Lawyer - Data Protection Officer

KARIN MALASPINA Lawyer - Data Protection Specialist

GERMANA MARRAFFA Data Protection Officer

GLAUCO RAMPOGNA

LEONARDO SCALERA Data Protection Officer

Editorial curators: **NATALIA ARTEMENKO, BARBARA CALDERINI, KARIN MALASPINA**

Table of contents

Please note that the paragraph numbers of this Response correspond to those of the Guidelines 01/2021 on Examples regarding Data Breach Notification adopted on January 14, 2021 and open for public consultation.

INTRODUCTION

by Leonardo Scalera

The EU General Data Protection Regulation 2016/679 (hereinafter, "**GDPR**") has brought a number of regulatory innovations that have determined organizational, operational and technological implications on the principal processes of personal data management within organizations. In particular, among other innovations, the GDPR imposes the obligation to manage security incidents resulting in personal data breaches, which requires the ability to analyze, verify and react within "tight" timings and, therefore, careful and precise prior planning activity.

Indeed, in the event of a personal data breach, it is mandatory to carry out accurate checks in order to determine whether compliance with the provisions of articles 33 and 34 of the GDPR (notification to the competent supervisory authority and to the subjects whose data have been breached) is required or, in any case, to keep track/records of the incident documenting the decision-making process that led to the decision not to notify the supervisory authority and the interested parties in accordance with the provisions of article 5 and recitals 74 (accountability principle) of the GDPR.

A data breach, or a personal data breach, is a security incident "*leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (article 4, no. 12 of the GDPR).

With regard to events that have occurred or may occur (threat) as a result of another unlawful or accidental event, the personal data breaches can be broadly classified into three types:

Type of Breach	Event / Threat
Confidentiality breach	Unauthorized or unlawful access or processing
	Unauthorized disclosure
Integrity breach	Unauthorized or accidental alteration
Availability breach	Accidental or unlawful loss or destruction
	Temporary or prolonged unavailability

These types are not mutually exclusive: a personal data breach can simultaneously concern confidentiality, integrity and availability. One of them or their combination can be implemented through purely technical activities, but can also derive from the "human factor" responsibility - conscious/voluntary or unconscious/unaware - or, as in this case, from a mix of factors.

Specifically, the most common causes leading to personal data breaches can be grouped as follows:

- malware (e.g., ransomware, crypto, botnet, banking trojan, RAT),
- phishing/social engineering,
- vulnerabilities,
- account cracking,
- DDos,
- multiple threats,
- human factor.[1]

[1] 2020 Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/dbir/

It should also be noted that the same type of personal data breach may have different severity, depending on the sector where the controller operates, the type of breached data or the number of subjects whose data have been breached (e.g., a personal data breach having the same characteristics will be managed differently depending on whether the controller operates in the healthcare sector or in the commercial sector).

For instance, the macro-sectors can be divided into the following groups:

- healthcare,
- financial sector,
- education,
- professional services,
- public authorities,
- retail,
- technology,
- industrial sector,
- hospitality,
- insurance,
- entertainment,
- non-profit,
- social media,
- others (mixed).

Based on the sector of activity and the type of data processed, it can, therefore, be necessary to integrate the security measures, as well as to adapt the actions following discovery of a breach, including the decision to notify or not to notify the event to the competent supervisory authority and to the interested parties.

Last but not least, one must consider the provisions of article 32 of the GDPR with regard to the nature, scope, context and purpose of the processing, but, above all, to the state of the art and the implementation costs for technical and organizational security measures to protect data and its processing.

Comments on assessment of the risks arising from a data breach and on advisable prior measures set out in the Guidelines

by Gianmarco Cenci

Comments on assessment of the risks arising from a data breach

The Guidelines 01/2021 on Examples regarding Data Breach Notification, version for public consultation (hereinafter, the "**Guidelines**"), appear an extremely useful instrument to assess the severity of a data breach and determine if a notification to the competent supervising authority (hereinafter, also the "**SA**") and to the data subjects is mandatory.

The Guidelines analyze different types of possible data breaches, opening with the type of loss or attack suffered by the data controller, moving on to recommendations on how to assess the severity of personal data breaches, and ending with a review of the security measures to be taken in order to prevent the event from occurring and, after the incident has occurred, to mitigate the severity of the data breach.

Assessment of the severity of personal data breaches seems to be the most relevant operation in order to determine what steps need to be taken next.

The data controller must decide if a notification to the SA is mandatory and a communication to the data subjects is necessary, and the Guidelines can help the data controller in taking such a decision.

When reading the Guidelines, we wonder if ENISA working document (v.10, December 2013)[2] "*Recommendations for a methodology of the assessment of severity of personal data breaches*" is an additional assessment instrument to determine the actual severity of a data breach and accordingly notify the competent supervising authority, as well as the data subjects concerned, and to quickly take the necessary mitigation measures.

The Recommendations underline that the data controller should always take into account, while assessing the severity of a personal data breach, three main criteria: Data Processing Context (DPC), Ease of Identification (EI), and Circumstances of the breach (CB).

These criteria do not seem very different from those outlined by the EPDB in the Guidelines: they all consider the category of the breached data (e.g. simple, behavioural, financial data, and special categories of personal data), the ease of identification of individuals, and the specific circumstances of the breach.

The methodology aims at defining the severity level of a data breach using the following formula:

SE (Severity) = DPC * EI + CB

While the DPC score is defined by evaluating the category of the data and the context of data processing (such as volume of data, special characteristics of the data controllers, those of the data subjects, public availability); the EI is a *"correcting factor"* since "*the lower the ease of identification is, the lower gets the overall score"*.

Loss of security (confidentiality, integrity, availability) and malicious intent (inferred from the nature of the data breach, it *"is a factor that increases the likelihood that the data is used in harmful way, since this was the initial purpose of the breach*") are listed under the CB.

Although this approach seems to overturn that of the Guidelines, which open with the type of data breach to make subsequent assessments, they actually take into account the same elements and lead to the same conclusions through a path that is not so different as it seems to be at first sight.

Therefore, it is necessary to consider how a method that defines the severity of a data breach in numerical terms can help the data controllers to become more aware of the severity of the data breach they have suffered.

This awareness may lead the data controllers to feel more comfortable in deciding what to do about the breach, including what mitigation measures to take, whether the notification to the supervisory authority is mandatory, and whether the data controller has to inform the data subjects about the breach.

Although the Guidelines never refer to the aforementioned Recommendations, we believe it would be a good idea to have such a methodology applied by both the data controllers and the supervisory authorities.

This would result in more verifiable data breach assessments and would help the data controllers, especially where they are small and medium-sized enterprises (SME), to comply with the requirements of the GDPR and at the same time be confident that they have acted accordingly.

Moreover, both the data controllers and the supervisory authorities may benefit from a more objective and less discretionary application of the law.

Comments on advisable prior measures set out in the Guidelines

We would like to highlight that some other issues would deserve further consideration, *e.g.* advisable measures listed in paragraphs 2.5, 3.4, 4.3 and 5.4.

These measures, however, do not relate to the actual data processing contexts or to the categories of the data processed or to their special nature. Moreover, the choice to select the most appropriate measures is left to the data controllers in accordance with the accountability principle.

[2] December 20, 2013, Data Protection Authorities of Greece and Germany, Clara Galan Manso, ENISA, Sławomir Górniak, ENISA https://www.enisa.europa.eu/publications/dbn-severity

Although the Guidelines state that the listed measures are only given by way of example, the data controllers might think they have to implement all of them in order to comply with their obligations under the GDPR.

Nonetheless, they may not realize in what context of processing a particular security measure should be implemented and in what context it is not so relevant.

A more detailed case study outlining the most appropriate measures based on the category of the data processed and the context of processing (including with regard to the ease of identification of the data subjects) could be more valuable to select, among those set out in the Guidelines, the security measures which the data controllers need to implement.

Specific security measures may be appropriate for the processing by the data controllers of certain categories of data in a given business area.

Other security measures might even be extremely strenuous in relation to the processing activities carried out by the companies operating in a different context.

Penetration testing would certainly be an adequate measure for a hospital processing health data of a very large number of individuals, but disproportionately burdensome for an agricultural company with few employees and clients.

Outlining the security measures which the data controllers must implement proportionally to the data processing operations, the category of the processed data, the context of the processing and the consequent risk to the rights and freedoms of natural persons, as well as the data controllers' financial resources would provide them with the means to comply not only with article 33 but also with article 32 of GDPR.

Brief observation on DPO and his/her/their role in data breach management

by Barbara Calderini

We would like to underline the crucial role played by the DPO (supported by the other competent functions) in the context of the process of management, understanding, analysis and report of an incident. Furthermore, in the initial phase of assessment of a data breach and in quantification of the severity of the risk, correct performance of his/her/their specific function is a decisive and determining factor.

Although article 39 of the GDPR does not expressly indicate among the tasks of the DPO that of providing advice on the event of security incidents, however, the non-exhaustive nature of the list contained in the same article does not exclude its presence among the tasks assigned to him/her/them by the data controller. Indeed, article 38 paragraph 1 seems to confirm such a task. Any intervention by the DPO should be specifically mentioned in the accident management report and in the acts of communication and notification to the supervisory Authority and to the interested parties.

RANSOMWARE and DATA EXFILTRATION ATTACKS

by Barbara Calderini, Glauco Rampogna

We share the purpose of these Guidelines that is to provide useful elements for management of accidental or malicious data breaches, highlighting the specific factors to be taken into consideration during the risk assessment strategy.

We are equally in favour of the type of suggested approach based on practical declination of the principle of "accountability" by design and, therefore, aimed both at preventing breaches and at identifying the danger of vulnerabilities. Indeed, despite the growing need to understand data breach incidents from a risk management perspective, there are still few verifiable models that show virtuous examples of risk

management and the related solutions which organizations can use to effectively manage data breach incidents.

In this regard, an interesting academic **study[3] by Freeha Khan, Jung Hwan Kim, Lars Mathiassen and Robin Moore** proposed an integrated risk management model that extends the body of knowledge on data breach management by identifying and updating conceptualizations of risks (elements) and resolutions (actions) of data breaches and by providing a basis for organizational responses to emerging data breach incidents (heuristics). We, therefore, would suggest a careful reading of this study in view of further investigations.

General additional recommendation

by Barbara Calderini

Regarding Ransomware attacks, **paragraph 16** of the Guidelines states: "*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*."

A ransomware attack can be classified as an availability breach, but under certain conditions it can also be a risk factor for the confidentiality of the data set concerned. Furthermore, from a proactive point of view, it is necessary to foresee and plan strategies for managing and communicating the risk of attack, also with regard **to loss of integrity**. Indeed, in those cases where the guarantee of confidentiality should be considered potentially compromised, particular attention must be paid to the risk of loss of integrity and correctness of the information concerned. It is, therefore, necessary to provide, where relevant, forms of notification, information and communication of the event which, even if only in case of reasonable doubt about the loss of data integrity resulting from the confidentiality data breach, can be promptly communicated and made comprehensible to the supervisory authorities and individuals concerned.

We would like to highlight the importance of drawing the attention of DPOs, where appointed, of data controllers and processors to the necessity to maintain a high level of awareness and update of operators both on the correct strategies of management and prevention of cyber risks and on specific trends of ongoing threats. This would help DPOs, controllers and processors to always keep one step ahead and to be prepared.

In particular, the use of two-factor authentication systems (2FA) on all platforms should become common practice. Microsoft research[4] from July 2019 reports that 99.9% of account breaches would have been stopped by multi-factor authentication. On this point we return to what is expressed in the recent revision of the NIST Guidelines[5].

Equally, it is suggested that physical apps or tokens be privileged over confirmation messages (with OTP code) via telephone line "in order to avoid SIM swapping problems, now widely used by cybercriminals".

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

by Glauco Rampogna

[3] https://www.sciencedirect.com/science/article/pii/S037872062030330X?casa_token=jE4k5v0e-kQAAAAA:MoiDCVn75c9AthULWwCHgX6ukSWwlOGXo2UuFE091HfbTLFhI0xayZmp9b0L8itdgF79X0OnZg

[4] https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

[5] https://pages.nist.gov/800-63-3/sp800-63-3.html

The Guidelines offer industry operators and stakeholders a reference point regarding the management of their activities to secure their data and IT systems.

Given the importance and wealth of practical examples of security measures to be applied to counter the effects of ransomware, **paragraph 49** suggests that backup strategies be integrated by explicitly using the term "offline", in accordance with the procedure called 3-2-1[6]. The motivation of this suggestion is due to the fact that a multitude of private and public entities of modest size still use on premise IT systems and do not have sufficient economic capacity or internet bandwidth for multilayer management of Cloud backups, while they could implement with few resources a proper backup procedure on removable physical media, which guarantee sufficient capacity even for an extended retention window of time.

The latest trends regarding ransomware threats show an intensification in attempts to encrypt entire virtualized systems[7], exploiting some flaws in the most widely used software at this time, Vmware, and result in the total loss of functionality and not only access to files and data. The seriousness of these threats includes the violation of the physical host of virtualization, to which onsite and offsite backup devices are often connected, making the massive deletion of all the backup storage feasible. In this sense, standard procedures provide for the application of disaster recovery based on offline copies and represent the only defense system for infrastructure recovery.

3. Data exfiltration attacks

by Barbara Calderini

In relation to the provisions of **paragraph 50**, we suggest that all cybersecurity developers and experts, in line with the recommendations already contained in these Guidelines, make a careful evaluation of the following indications given by the best exponents of the sector (to which we would like to refer for a more thorough understanding) whose in-depth analysis is available here[8].

Structured Query Language (SQL) injection and Cross Site Scripting Attack (XSS) are two most common application-level attack techniques for defacing a website's security, manipulating or deleting its content by injecting strings of malevolent code. The danger resulting from it is extremely insidious.

Indeed, it can go as far as to threaten the security of critical infrastructures. It is sufficient to remind of a recent incident in Oldsmar, Florida (a water treatment incident).

The FBI in a notice (shared on Twitter[9] by Eric Geller of POLITICO) said that "the attack" likely "exploited an old Windows 7 operating system and weak password security as they (or he, or she) gained access to the TeamViewer software in use at the facility. The Bureau and the US Secret Service have joined state and local law enforcement in the investigation. No suspects have so far been named, or arrested".

These are the fundamental recommendations proposed:

- Use multi-factor authentication;
- Use suitably strong passwords to protect Remote Desktop Protocol (RDP) connections;
- Ensure that antivirus, spam filters and firewalls are up to date, configured correctly and protected;
- Check your network configurations and isolate computer systems that cannot be updated;
- Check your network for systems using RDP, closing unused RDP ports; applying two-factor authentication where possible and logging RDP access attempts;
- Use control log for all remote connection protocols;
- Train users to identify and report social engineering attempts;
- Identify and suspend the access of users who show unusual activity;
- Keep your software up to date.

[6] https://www.veeam.com/blog/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html
[7] https://www.zdnet.com/article/ransomware-gangs-are-abusing-vmware-esxi-exploits-to-encrypt-virtual-hard-disks/
[8] https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
[9] https://twitter.com/ericgeller/status/1359312457299329029

Additional defenses:

- Enforcing Least Privilege;
- Performing Whitelist Input Validation as a Secondary Defense.

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

by Barbara Calderini

Observation no.1 - Security experts in the valuable guide called **OWASP Cheat Sheet**[10] suggest using modern hashing algorithms such as **Argon2id**, **PBKDF2** or **Bcrypt**, which automatically embed the protection string known as "*salt*".

The *salt* should be at least 16 characters long and encoded with a secure character set such as hexadecimal or Base64.

The NIST guidelines[11] require that passwords be *salted* with at least 32 bits of data and hashed with a one-way key derivation function such as Password-Based Key Derivation Function 2 (PBKDF2) or Balloon. The function should be iterated as much as possible (at least 10,000 times) without harming server performance.

In order to protect the confidentiality of the access credentials, it is considered useful to carefully evaluate, especially in the most delicate cases or those where the available algorithms are legacy ones such as MD5 and SHA-1, the opportunity to proceed with the combined use of the two "***salt and pepper***" components. The purpose of *pepper* is to prevent an attacker from cracking any hash if he/she/they only accessed the database, for example, by exploiting a SQL injection vulnerability or by having obtained a database backup.

A good practice is that a *pepper* is at least 32 characters long, generated randomly using a secure pseudorandom generator (CSPRNG), archived and stored securely.

Experts also suggest an alternative and equivalent approach to *pepper* consisting of password hashing (in particular one-way hashing) followed by encrypting the hashes as a function of symmetric decryption key.

In this context, we would also like to bring your attention to the **study**[12] conducted by **Wenjie Bai** and **Jeremiah Blocki** focused on **DAHash (Distribution Aware Password Hashing)**, *i.e.* "*a novel mechanism which reduces the number of passwords that an attacker will crack. Our key insight is that a resource-constrained authentication server can dynamically tune the hardness parameters of a password hash function based on the (estimated) strength of the user's password.*"

The intuition of the scholars is based on the fact that a server of Resource-constrained authentication can dynamically adjust the hardness parameters of a password hash function based on the (estimated) strength of the user's password. To this end they introduce a "*Stackelberg game to model the interaction between a defender (authentication server) and an offline attacker. The model allows the defender to optimize the parameters of DAHash e.g., specify how much effort is spent to hash weak / moderate / high strength passwords. They use several large scale password frequency datasets to empirically evaluate the effectiveness of differentiated cost password hashing mechanism. They find that the defender who uses the mechanism can reduce the fraction of passwords that would be cracked by a rational offline attacker by around 15%.*"

Observation no.2 - We would like to draw your attention to another useful suggestion relating to the correct setting of the ***work factor***.

[10] https://cheatsheetseries.owasp.org/
[11] https://pages.nist.gov/800-63-3/sp800-63-3.html
[12] https://arxiv.org/abs/2101.10374

A ***work factor*** indicates the number of iterations of the hashing algorithm that are performed for each password. Experts recommend "*finding a balance between safety and performance*". Higher work factors would make hashes harder for an attacker to crack, but would also make the process of verifying a login attempt slower. If the work factor is too high, it could degrade application performance and could also be used by an attacker to perform a denial of service attack by making a large number of logon attempts to exhaust the server's CPU.

"*As a general rule, computation of a hash should take less than a second, although on high-traffic sites it should be significantly less than this*."

Finally, it is very important not to be tempted by the possibility of writing custom cryptographic code such as a hashing algorithm, if not as a stylistic exercise.

Observation no.3 - The length of the password would also have its own weight in the mitigation of the risk in question: the **OWASP Cheat Sheet**[13] suggests that it should be 64 characters for Bcrypt (due to limitations in the algorithm and implementations) and between 64 and 128 characters for other algorithms.

In particular, the **NIST Password Guidelines**[14] appear useful: the NIST 800-63B password Guidelines originally published in 2017 were updated in March 2020 in "Revision 3" or "SP800-63B-3.

They are considered[15] the most influential standard for creating secure passwords by many password cracking experts. Each organization should disseminate knowledge and implementation thereof.

For a useful in-depth analysis of the security measures to prevent credential stuffing and password spraying attacks, we also suggest careful examination of the study **Credential Stuffing Prevention Cheat Sheet**[16] from which one can take useful recommendations on management and remediation.

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

by Glauco Rampogna

Paragraph 70 of the Guidelines suggests that the list be integrated with the consultation of the OSINT tools made available for a continuous verification of a possible breach of email accounts. This suggestion is motivated by the fact that digital identity theft, in these Guidelines associated with social engineering, occurs very often by taking possession of the email account and subsequently resetting the access passwords to portals and websites. In addition, given the availability of cloud storage associated with one's email account, it is common practice to use one's own inbox as a starting point for corporate document repositories, and this allows an attacker possible access to corporate data also located in the cloud.

INTERNAL HUMAN RISK SOURCE, LOST OR STOLEN DEVICES, PAPER DOCUMENTS and MISPOSTAL

by Germana Marraffa, Leonardo Scalera, Salvatore Coppola

[13] https://cheatsheetseries.owasp.org/
[14] https://pages.nist.gov/800-63-3/sp800-63-3.html
[15] http://www.cs.umd.edu/~jkatz/security/downloads/passwords_revealed-weir.pdf
[16] https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

The human factor (which is almost always about the persons authorized to process data) plays a particularly important role in the context of numerous studies dedicated to the causes of data breach and has always been considered a “weak link” among the security measures (whether cyber or not).

In the cases of personal data breaches deriving from viruses, ransomware, theft of logins and passwords, etc., it often happens that a large share of responsibility is attributed to the human factor. This is due to poor attention, lack of knowledge, lack of specific training or, sometimes, voluntary malicious conduct.

Basically, in almost all these cases, a constant and, as much as possible, continuous training of the personnel authorized to process data is undoubtedly necessary, in order to increase awareness of the actions taken during the processing activities, as well as of possible consequences of the actions that go outside the operating instructions provided by the data controllers or, ultimately, of deliberately malicious conduct.

Among the preventive measures, a theoretical training must be accompanied by practical tests and verifications. For instance, these can be: “testing” of personnel with actions designed to simulate “risky” events aimed at verifying the response to such events and, if an error is detected, the ability to react and implement the provisions of the specific policies/regulations adopted by the data controller in order to trigger a quick and as precise as possible response to a possible breach.

Indeed, in case such an event occurs, the time factor is of utmost importance both from the perspective of implementing any measures necessary to further mitigate any risks for the persons whose data have been breached and of timing related to any communication to the supervisory authority (and, if required, to the interested parties).

There are also a number of activities within the data controller’s structure where the human factor becomes decisive for a data breach, such as, for example, sending of communications (both by electronic means and not) outside the organization.

The same rules applicable for evaluation of the necessity to notify the supervisory authority and the interested parties (number of subjects concerned, nature of data concerned, preventive security measures or measures to mitigate the possible adverse effects, risks to the freedoms and rights of the subjects concerned, etc.) apply to this matter as well.

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

by Germana Marraffa

During the forty-first International Conference of Data Protection and Privacy Commissioners (ICDPPC) held in 2019, more than 120 intervened authorities adopted six resolutions, including one on the role of human error in personal data breaches, highlighting the necessity of an adequate training of personnel, further measures to mitigate the risk and establishment of a global archive to keep track of breaches.

It seems clear that the first tool to mitigate the risks due to human errors can only be correct and periodic training which should be seen as a moment to raise awareness of the employees, as well as an opportunity to design a corporate culture where privacy and security become organizational priorities. This training must necessarily be accompanied by safety measures tailored to various company realities, which, therefore, cannot be separated from a substantial and factual assessment of the limits of knowledge and technical know-how of each resource[17].

[17] The Guidelines 01/2021 on Examples regarding Data Breach Notification: 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.

A useful method for pondering the different behavioural approaches of employees and organizing a more targeted training may be the **Pen Test** which can reveal inappropriate behaviour of employees or non-compliance with company security policies that make the defence system vulnerable.

In some instances, the events relating to personal data breaches can be silenced by employees who (in some cases due to a poor awareness of the higher risks deriving from the lack of prompt reporting, in others voluntarily concealing it in order to avoid reprimands) silence the event causing to the controller greater damage by not allowing him/her/them to immediately implement the measures aimed at minimizing the risks and assessing the necessary measures[18], thus mitigating the risk factor.

Example: sending an e-mail containing financial data belonging to several interested parties

An interested party, client of an intermediary, reports a data breach. The person received a report containing, in addition to financial information relating to his/her/their debt position, the information relating to other clients of the same intermediary. The Data Controller, therefore, initiates a brief internal investigation and discovers that the personal data breach occurred a month before and that the person authorized to perform that specific activity concealed the event, which had involved other customers whose data were in the same document. The Data Controller informs the other interested parties of the breach, submits notification to the supervisory authority (*Garante*) of the breach and updates the data breach register.

Organizational and technical measures for preventing / mitigating the impacts

The measures to effectively mitigate the risks of such a breach are limited.

Although the controller requested deletion of the message, he/she/they cannot force the recipients to do so, and consequently, cannot be certain that they fulfil the request.

All the three following actions below should be taken.

Actions necessary based on the identified risks		
Internal register	Notify SA	Communicate to data subjects
✔	✔	✔

The letters of appointment drawn up pursuant to article 29 of the Regulation are of utmost importance. In segmenting different areas of processing, they must clearly set out the responsibilities of the employee authorized to process the data in the cases where he/she/they, while performing his/her/their functions, commits errors and, consciously or not, decides to conceal them from the Data Controller, not allowing the same to implement the necessary measures to mitigate the risks of the breach which can potentially become more dangerous if not properly notified to the supervisory authority.

The Data Controller, giving specific and clear instructions in a letter of appointment, should also highlight how non-compliance with the personal data protection rules not only constitute a contractual breach but may also lead to civil or criminal liability with consequent application – whenever the conditions are not met – of the related sanctions as well as any compensation for damage caused to third parties. This is particularly important in the case of breaches not promptly reported and in violation of the data breach procedure that the Data Controller must have appropriately implemented, including in order to be able to document any personal data breach, its consequences and the measures taken to remedy it, as well as to allow the supervisory authority to verify compliance with the provisions of the GDPR.

This approach obviously implies the publication, within the corporate structure, of clear and correct policies governing the methods for sending letters/e-mails.

Remote working

[18] The Guidelines 01/2021 on Examples regarding Data Breach Notification: 3.2.2 CASE No. 06 – Mitigation and obligations. 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.

If the Data Controller concludes with his/her/their employees home working contracts, he/she/they must first assess the risks and draw up internal policies that clearly govern the protection of personal data when such data is processed remotely: for example, production of prints containing personal and/or financial data, and their disposal.

In fact, if we consider that many data breaches have occurred within working environments with good security measures and system administrators present on site, the risk can increase in the case of remote working where an employee uses his/her/their own PC, perhaps, used by several people in his/her/their household, a home network, which means unsecured wi-fi networks, and has few cyber security skills.

In this case, the Data Controller must update his/her/their internal policies, establishing limitations and requesting use of more reliable access methods, such as an OTP system or, anyway, a more secure and reliable access method than simple use of a password associated with a user name.

The organizational and technical measures to prevent/mitigate the risk impacts in case of remote work must necessarily be listed in a sort of *vademecum* that the home worker (*smart worker*) must respect. Here are some basic rules, by way of example:

- use as “home network” only your own or, in any case, the networks that have proven security (avoid “free” wi-fi or unknown or public hot-spots);
- be sure that access to the home network is protected by adequate login and password (*i.e.* network name that cannot be associated with a person and a sufficiently complex password) and, if necessary, check that the router/connection devices are secure;
- take every care to prevent unauthorized persons present in the off-site location from accessing the data;
- block the computer in case of quitting the workstation, even for a very limited period of time;
- if devices provided by the data controller are not used, it is necessary to verify that the same security measures adopted on the company workstations are respected (such as, for example, a reliable antivirus system always active, adequate access login and password);
- avoid use of social networks or other easily hackable social applications;
- use “security measures” on PCs or tablets, such as, for example, the privacy-screen that prevents side view, not only for reasons of confidentiality, but also for those of data flow;
- during business contacts, avoid revealing over telephone personal information that may be used to breach the system;
- be careful not to send corporate information or professional secrets by mistake to third parties who are not authorized to receive them;
- avoid opening suspicious attachments;
- an agile employee must pay the utmost attention to the origin of the e-mail messages, verifying if the company to which the sender belongs really exists by looking for confirmation on web or social media, the content of the text (as from a simple but careful reading it is possible to detect logical inconsistencies, often due to automatic translators), as well as the presence of unknown links or suspicious attachments. In case of doubt about any of these situations, the employee must ask his/her/their IT team what to do, avoiding any own initiative;
- in the event of anomalies or blocks due to viruses or malware, the home worker (*smart worker*) must suspend all operations, shut down the system and its applications, and immediately inform the IT team;
- at the end of the daily work performance, keep and protect any documents printed, providing for their possible destruction only after you have returned to your usual place of work;
- if, however, at the end of the work it is necessary to keep at home paper material containing personal data, the same must be placed in cabinets, drawers or lockers.

Finally, as a last but not least precaution, we consider it essential to appoint a System Administrator, who, although not expressly provided for by the GDPR, plays an extremely delicate role, given the technical peculiarities. The System Administrator designs, develops and manages the network infrastructure, servers, software and basic application services, often dealing with the security and protection of data and resources. Furthermore, he/she/they provides technical (help desk) and IT support on software and hardware. When necessary, he/she/they plays a proactive role in notifications of security

breaches and data breaches, notifying the DPO of any anomalies discovered on malfunctions or security risks. He/she/they is responsible for the activities carried out and the consequences deriving from a malfunction of the network, as well as supports the DPO and the persons authorized to process data on the IT aspects in the ordinary course of business.

The System Administrator usually coincides with the IT manager and is the one who, in performing purely technical tasks (such as data saving, organization of network flows, management of storage media, installation and updating of antivirus and firewalls, management of login, passwords and authentication, authorization and hardware maintenance systems), has a privileged or accidental access to a considerable amount of company information that can be considered in all respects processing of personal data.

In the letter of appointment of the System Administrator, it is therefore advisable to insert a clause on his/her/their availability which, although expensive (as he/she/they must necessarily be remunerated), can become a precious lifesaver, useful for avoiding shipwreck resulting from a data breach following a cyber-attack that mostly occurs outside of normal working hours and the damages of which can become incurable if not tackled immediately and competently.

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

by Salvatore Coppola

A correct identification of the "personal data breach" (or simply "data breach") should necessarily be a key point in the protection of personal data. A thorough knowledge of this matter contributes in a decisive way to timely and promptly address the harmful consequences for the data subjects.

In this regard, article 29 Working Party already analysed the relevant sections of the GDPR and published in October 2017 general Guidelines on personal data breach notification[19].

The Guidelines currently under consultation, therefore, as highlighted in the introduction, arise from the need to provide a guide oriented to practice and cases which appear more probable and attributable to personal data breaches pursuant to article 33 of the GDPR.

The purpose is, therefore, to facilitate the data controller's task in recognizing a personal data breach.

Therefore, it is very important to consider the situations where, due to the "quantity and quality" of the breached personal data, it is necessary to identify "minimal"[20] cases in order to warn against interpretations that would leave persons without adequate protection.

In particular, we refer to **Case no. 11** of the said Guidelines under consultation: "*Stolen material storing non-encrypted personal data*".

This case relates to a personal data breach, meaning a "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (article 4 par. 12) of the GDPR), where an electronic notebook of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and dates of birth more than 100,000 customers who, thus, became affected by the data breach. Special categories of personal data and personal data relating to criminal convictions and offenses, as defined in articles 9 and 10 of the GDPR, were not affected.

[19] See article 29 Working Party: *Guidelines on Personal data breach notification under Regulation 2016/679 adopted on 3 October 2017 as last revised and adopted on 6 February 2018*, WP250rev.01

[20] The author is aware that due to the principle of "accountability", with particular regard to the technical and organizational measures that the controller must adopt in order to guarantee and be able to demonstrate that the processing is carried out in compliance with the GDPR, it is necessary to abandon the concept of "minimum" in favour of that of "adequate", precisely because of greater "accountability" – in a narrow sense – of the data controller.

The personal data breach was made possible due to the absence of the necessary measures aimed at ensuring a level of security appropriate to the risk, as required by article 32 of the GDPR.

The indication of such a "considerable" number of customers "affected" by the breach of their personal data – given the discretionary definition of the concept "large scale" in other contexts – may induce data controllers (and processors) to underestimate and, therefore, not communicate personal data breaches that affect a smaller number of interested parties. In fact, how would a "hasty" interpreter, who is not very sensitive to the data protection issues, evaluate a data breach that affects 10,000 customers? Or 1,000? Or 100?[21]

Indeed, it would seem more functional to the aforesaid purpose to refer to the personal data breach consisting in the loss of a device that contains personal data of at least a smaller number of interested parties.

There is no doubt that the example provided in the previous Guidelines WP250rev.01 remains even clearer for our purpose: "1*. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost*".[22]

Finally, among the indications referred to **in paragraph 5.2.1.** ("*Prior measures and risk assessment*") no "explicit" reference is made to pseudonymisation, the main security measure among the basic ones set out in article 32, par. 1, of the GDPR.

The pseudonymisation technique[23] and its ability to ensure the non-identifiability of the data subjects whose personal data contained on the stolen device should deserve greater evidence, "at least" to limit the risk of disclosure of such data to unauthorized persons, since the case refers to a stolen device containing non-encrypted data.

In conclusion, it is always advisable to call the attention of the data controller (and processor) to the adoption of procedures suitable for testing, verifying and regularly evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.

6.1 CASE No. 13: Snail mail mistake

by Leonardo Scalera

Commercial sector, incorrect delivery of an order with the related documents containing personal data of two subjects.

In this case, the subjects concerned are few and the data in question relate to the delivery, therefore, ***it is not considered necessary to notify the supervisory authorities and the interested parties, but only to register the event*** after requesting the recipients to destroy any copies of the data in their possession. It is advisable to implement a system to double-check not only item codes in combination with customer codes, but also order and package addresses.

If the set of data sent by mistake contained personal data belonging to special categories (*e.g.*, medical reports relating to particular pathologies), the scenario described above would have changed: the

[21] The GDPR does not unequivocally define what "large-scale" processing means. With regard to the data protection impact assessments, recital 91 includes in this definition, in particular, "*large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk*". As for the appointment of a Data Protection Officer, article 29 Working Party recommended to consider the following factors: 1) the number of data subjects concerned – either as a specific number or as a proportion of the relevant population; 2) the volume of data and/or the range of different data items being processed; 3) the duration, or permanence, of the data processing activity; 4) the geographical extent of the processing activity (see *Guidelines on Data Protection Officers ('DPOs') adopted on 13 December 2016 as last revised and adopted on 5 April 2017*, WP 243 rev. 01).
[22] See article 29 Working Party, WP250rev.01, p. 12.
[23] See Enisa, Pseudonymisation techniques and best practices, 2019, p. 23.

same breach event would have implied the necessity to notify the supervisory authorities and the interested parties.

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

by Leonardo Scalera

An e-mail message was sent to a large number of recipients; a document attached to this e-mail contained by mistake a list of the recipients and their personal data, including “sensitive” one.

In this case there is a large number of subjects concerned, the “sensitive” data, and the only available possibility for the controller is to contact the recipients requesting to delete the data erroneously received (an action which cannot be certain). In this case, since the controller cannot be sure that the data will be deleted, ***it is necessary to notify the supervisory authority and the interested parties in addition to the internal records***.

It would be necessary to adopt more stringent rules in order to mitigate the risk of email mistakes, such as lists prepared and checked in advance or pre-set messages with checked attachments, closed mailing lists for delivery with a lower risk of mistake, setting delay time for cancellation/modification of messages, etc.

In this case, a more careful evaluation of security measures and stricter policies on mail delivery systems would have considerably mitigated the risks deriving from a human error, so that it would not have been necessary to notify the supervisory authorities and the interested parties, but only to register the event and the solutions adopted on the internal records.

OTHER CASES: SOCIAL ENGINEERING

7.1 CASE No. 17: Identity theft

by Karin Malaspina

The **case illustrated under no. 7.1)** presents a high level of risk, so the “appropriate” authentication measure of identity should maintain a high level of protection. In this regard, two aspects should be evaluated and considered: patterns of data that can be processed as a result of authentication and different areas in which the stolen personal data can be used.

Critical data is any form of personally detectable information, unique to each person, such as: birth certificate; social security number; taxpayer identification number; insurance policy number; bank account number; credit card number; driver’s license number; employer identification number.

An identity thief would use physical data or any information he/she/they can collect from a person’s mail or from trash to get the critical data.

When investigators want to find out about a suspect, the first thing they look at is the person’s habits. Identity thieves know about this tactic, and use it to frightening effect. Some forms of physical data include: residential address; the tag of pets; unsolicited mail (brochures); account numbers for utilities such as water, gas, and internet; billing statements.

Finally, public data are trickier to handle because the information is available to everyone. Some forms of public data include: telephone numbers; employer name and address; doctors and medical providers; email address; social media; license plate.

There are several types of identity theft, including:

- Phishing - Cyber criminals send fraudulent emails or texts that may look legitimate. The links in these emails or texts may be used to download malicious software — malware, for short. The software may be able to mine users' computers for personal information and send it to a remote computer. Cybercriminals use this information to commit identity theft or sell it on the dark web.
- Skimming - Credit card skimming happens when criminals replace card readers with a counterfeit device at cash counters or other point-of-sale systems, such as those at grocery stores, coffee shops, or gas stations. This device captures data contained in the magnetic strip of credit cards and debit cards and passes it to the skimmer. Sometimes, a small camera is set up to capture entries like ZIP/postal codes and ATM PINs. With information like credit card or debit card numbers, names, postal codes, or ATM PINs, criminals may be able to make fraudulent purchases or withdraw cash in the account holder's name.
- Wi-Fi hacking - Some public Wi-Fi connections are unencrypted. This could give criminals a chance to snoop on data traveling. If a user's device has software vulnerabilities, cybercriminals may be able to inject malware to help them gain access to the personal data. Cybercriminals sometimes create fake Wi-Fi hotspots with names that sound like a legitimate network. Identity thieves may be able to view and exploit the information passing through the rogue network.
- Dumpster diving - Identity thieves may steal mail and patch together with the personal information to commit identity theft. They could get important details like bank account numbers, health insurance details, or credit card details by stealing mail. They might be able to create a new identity if they access key information.
- Phone scams - Fraudsters may call a user on the phone, claiming to be from a bank asking for money.
- Data breaches - After a data breach, users' personal information could be at risk of being sold on the dark web. Sometimes a data breach puts at risk the personal information of millions of people.
- Malware - Criminals use different techniques to install malware on another person's device. Malware could allow the criminal to access the device and information stored on it. Malware types include viruses, spyware, trojans, keyloggers.
- Mail theft - Thieves may sift through a person's mail in hopes of finding personally identifiable information. For instance, they might find a credit card statement with account number, a tax form with social security or tax identification number, or other pieces of information that can help them commit identity theft.
- Child ID theft - Identity thieves can use a child's social security or tax identification number to open financial accounts, apply for government benefits, apply for loans, and to apply for an apartment. The person whose identity was stolen might not know about the fraud until they apply for loans or other types of credit as an adult.
- **Tax ID theft** - Tax-related identity theft occurs when someone uses personal information/personal data , such as social security or tax identification number, to file a tax return to collect a tax refund.
- **Medical identity theft** - Someone poses as another person to obtain free medical care.
- **Synthetic identity theft** - is a type of fraud in which a criminal combines real (usually stolen) and fake information to create a new identity, which is used to open fraudulent accounts and make fraudulent purchases. Synthetic identity theft allows the criminal to steal money from any credit card companies or lenders who extend credit based on the fake identity.
- **Criminal identity theft** - A criminal poses as another person during an arrest to try to avoid a summons, prevent the discovery of a warrant issued in their real name, or avoid an arrest or conviction record.

Mitigation measures

There are several identity theft protection services that help people avoid and mitigate the effects of identity theft. Typically, such services provide information helping people to safeguard their personal information; monitor public records and private records, such as credit reports, to alert their clients of

certain transactions and status changes; and provide assistance to victims to help them resolve problems associated with identity theft.

In addition, some government agencies and nonprofit organizations provide similar assistance, typically with websites that have information and tools to help people avoid, remedy, and report incidents of identity theft. Many of the best credit monitoring services also provide identity protection tools and services.

Measures to prevent these crimes necessarily require interaction between users and companies that manage their personal data.

The companies/organizations should take the following measures:

- adopt a form of combined control, shared between the interested holder and the company / organization.
- adopt policies to prevent these crimes, and Guidelines about identity theft, which describe different cases.
- make available to users a reporting service through channels (former dedicated telephone line, active 24 hours a day) and standard forms, which facilitate exercise of a request for protection by users and allow to intervene as soon as possible [24].
- complete information about consumers' rights and the attention they should give to avoid case identity theft.
- implementa form of authentication which would result in a high degree of confidence.
- so that effective authentication be valid and compliant, it should combine different type of personal data required in order to consider validly confirmed authentication.
- introduce an out-of-band multi-factor authentication method, which would resolve the problem, and require different kinds of personal data, including personal information that the only owner may know.
- adopt a policy to verify in different steps the same identity between the person who requires access and the authenticated user.
- provide a multi-access system that requires not only public personal data, which can easily be stolen, but also other data, generated ad hoc through devices of which the owner only has access.
- multi-access system could give a chance to the users to detect alert signals in the event that an identity theft incident is taking place, [as he will be involved at least in one of the step chains provided for user profile authentication][25].

The users should take the following measures:

- create unique, complex passwords, for each account and device. A strong password includes a dozen letters, numbers, and symbols; or create a long passphrase, which would be hard for a criminal to guess, but easier for you to remember.
- enable two-factor authentication on all accounts that offer it.
- never give out personal information — especially on phone calls.
- not share documents before throwing them away. These might include mail, receipts, bills, and any other paperwork that contains sensitive information.
- choose paperless billing when possible, so account information doesn't get sent to mailbox.
- leave social security card, medicare card, and debit and credit cards in a safe place at home.
  Use websites that are secure. The URL will start with an "https" (the "s" stands for "secure").
- check financial accounts often and keep tabs on credit reports to look for changes that were not made by the holder.

[24] Identity theft recovery step - FEDERAL TRADE COMMISSION, "Consumer.ftc.gov"
[25] "IT threat evolution Q3 2019. Statistics" November 29, 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/
"FOAM JACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month" August 2019.
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf
"Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web"VMWare.
https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

- do not click links, open attachments, or respond to emails from unfamiliar or untrusted sources. These may contain malware.
- set up alerts on banking and credit card accounts.
- never share the personal data with anyone unless necessary and stored in a secure, physical location like a home safe or safety deposit box.
- safeguard personal information by using a shredder on all mail before throwing it out.
- update anti-virus software and anti-spyware programs. Most types of antivirus software can be set up to make automatic updates. Spyware protection is any program that protects personal information online from malware.

We thank you for your attention and remain available for any further discussion or clarification.

Yours faithfully,

dataTENET