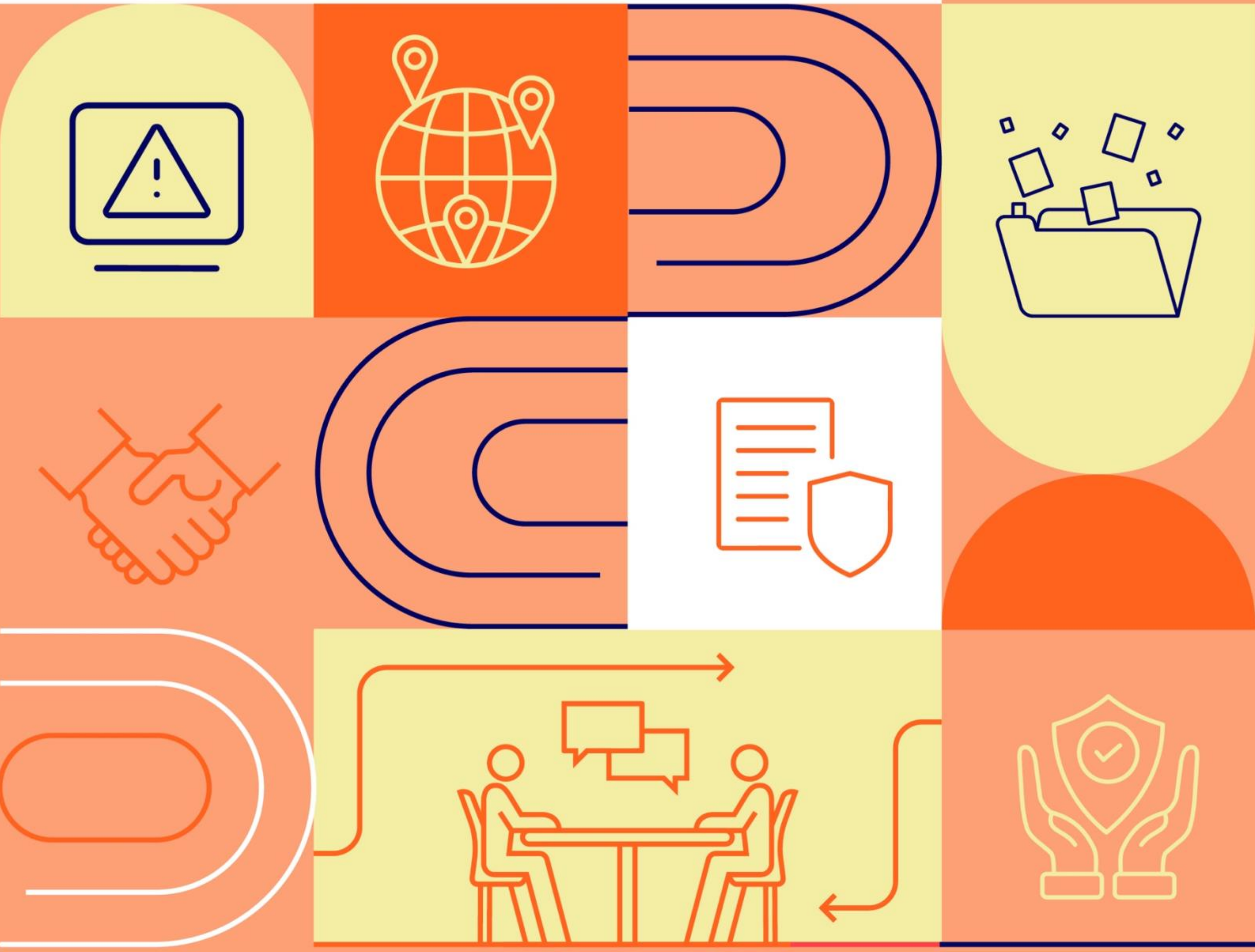
Thematic document

# Security of Processing and Data Breach Notification

Eleni Kosta

Professor of Technology Law and Human Rights, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University



Final – 27 November 2023

# Legal studies by external providers

The EDPB may commission contractors to provide legal studies on specific topics. The views expressed in the legal studies are those of their authors and they do not necessarily reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in the legal studies. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use which may be made of the information contained in the legal studies. Some excerpts may be redacted from the legal studies as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

Thematic case digest

# One-Stop-Shop mechanism and decisions

## Foreword by EDPB

This thematic digest looks at a selection of examples of final One-Stop-Shop decisions taken from the EDPB's public register. The Register was consulted between 10 July and 31 August 2023. The thematic case digest analyses decisions relating to Articles 32 (security of processing), 33 (notification of a personal data breach to the supervisory authority) and 34 (communication of a personal data breach to the data subject) of the General Data Protection Regulation (GDPR). The OSS thematic digest is a valuable resource to showcase how Supervisory Authorities (SAs) work together to enforce the GDPR. It offers an exceptional opportunity to read final decisions taken by, and involving, different SAs relating to the security of processing and personal data breach notifications. The OSS thematic digest was produced within the framework of the EDPB Support Pool of Experts, a strategic initiative of the EDPB that helps Supervisory Authorities increase their capacity to supervise and enforce the safeguarding of personal data.

## The One-Stop-Shop Mechanism explained

The One-Stop-Shop (OSS) mechanism demands cooperation between the Lead Supervisory Authority (LSA) and the Concerned Supervisory Authorities (CSAs). The LSA leads the investigation and plays a key role in the process of reaching a coordinated decision between the SAs. The LSA investigates the case while taking into account national procedural rules, ensuring that individuals can exercise their rights. It shall cooperate with the other Supervisory Authorities concerned and endeavour to reach consensus. In particular, it can gather information from another SA via mutual assistance or by conducting a joint investigation. The Internal Market Information system (IMI) supports the authorities in exchanging relevant information. The LSA then prepares a draft decision, which it submits to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. In such a case, the LSA must adopt its final decision on the basis of the EDPB's binding decision.

# Table of contents

# 1. Scope and methodology

This report analyses the decisions adopted by Supervisory Authorities (SAs) pursuant to Article 60 GDPR[1] under the One Stop Shop mechanism in the field of security of personal data processing and personal data breaches. The dataset was extracted from the register of final one stop shop decisions made publicly available online by the European Data Protection Board (EDPB).[2] The register was consulted between 10 July and 31 August 2023.

The relevant decisions were initially filtered using the search engine on the EDPB website by setting Article 32 GDPR as the main legal reference. The 62 selected decisions were then analysed to identify the most significant ones. The same process was adopted regarding Articles 33 GDPR and 34 GDPR. The search returned 54 cases for the former and 38 cases for the latter. As, due to the nature of these Articles, they were often found in the same cases, for the purposes of this report 90 decisions were analysed ("Final One Stop Shop Decisions"). In Annex I, a list of these Final One Stop Shop Decisions can be found, where it is clearly indicated which Articles (32, 33 or 34 GDPR) are relevant in each decision. These decisions were adopted between January 2019 and June 2023.

The analysis included in this report depends on the level of detail of the final decisions. For example, the description of the security measures or other factual findings may be more or less detailed depending on the adopted final decisions, which has an impact on the content of this report. In addition, the final decisions refer in certain cases to other non-public documents that were exchanged during the procedure and therefore could not be analysed as part of this report. The analysis often refers to guidance documents adopted at national level cited in the decisions. Since the majority of such guidance documents have been updated since the adoption of the relevant decisions, the references link to the current version of these documents in order to provide a clear picture of the state of the art.

Most of the decisions offer interesting insights on the interpretation and application of Article 32 GDPR by SAs in concrete situations. In addition, the decisions on Articles 33 and 34 GDPR are often linked to security of processing and applied altogether with Article 32 GDPR. For this reason, this report does not follow an analysis of the decisions for each of these three Articles. It rather makes

[1] Regulation (EU) 2016/679 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 (General Data Protection Regulation (OJ L 119, 4.5.2016, p.1).

[2] The EDPB database is available at https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en, last accessed 31.08.2023.

a thematic analysis of the most important topics that have been dealt within the One Stop Shop mechanism.

# 2. Setting the scene on the regulation of security of personal data in the GDPR

## 2.1 Articles 32, 33 and 34 GDPR on the security of personal data

Section 2 of Chapter IV GDPR regulates the issue of security of personal data and comprises of three distinct Articles: Article 32 on security of processing, Article 33 on the notification of a personal data breach to the supervisory authority and Article 34 on the communication of a personal data breach to the data subject. This section will provide a brief overview on these three Articles. Article 32 GDPR contains fundamental rules for ensuring the security of personal data processing, by establishing an obligation for both data controllers and data processors to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk". The analysis of the Final One Stop Shop Decisions will provide insights on how SAs interpret these obligations in concrete situations, such as how to protect organisations against hacking, how to ensure meaningful and robust encryption or how to build strong passwords, to name just a few.

In case of a personal data breach, following the obligations established in Article 33 GDPR, the data controller shall notify the competent supervisory authority of the breach, "without undue delay" and, "where feasible", "not later than 72 hours after having become aware of it". In case the notification takes place after the period of 72 hours, it shall be accompanied with reasons for the delay. A notification to the supervisory authority is not required when the personal data breach is unlikely to result in a "risk to the rights and freedoms of natural persons". The analysis of the Final One Stop Shop Decisions sheds some light on when a notification is required or not.

Finally, Article 34 GDPR establishes an obligation for data controllers to communicate the personal data breach to the affected data subjects "without undue delay", when the personal data breach is likely to result in a "high risk to the rights and freedoms of natural persons". The analysis of the Final One Stop Shop Decisions brings further clarity on when a communication to the data subjects is required.

## 2.2 The EDPB guidelines on data breach notifications

The issue of data breach notifications has been extensively dealt with, initially by the Article 29 Working Party and then, following the entry into force of the GDPR, by the European Data Protection Board (EDPB). The EDPB endorsed the previous Guidelines on

Personal data breach notification published by the Article 29 Working Party.3 In order to provide some guidance on the practical issues that arise in relation to data breach notifications, the EDPB published in December 2021 a new set of guidelines, which are meant to be "practice-oriented, case-based guidance, that utiliz[e] the experiences gained by SAs since the GDPR is applicable".4 Finally in March 2023 the EDPB published the (second version of the) EDPB Guidelines on personal data breach notification5, which is a "slightly updated version"6 of the WP29 Guidelines on personal data breach notification. This document establishes that "[a]ny reference to the WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) should, from now on, be interpreted as a reference to these EDPB Guidelines 9/2022"7. The updated EDPB Guidelines 9/2022 include – among others – a new section on the notification requirements concerning personal data breaches affecting non-EEA establishments.8 The 2023 EDPB Guidelines are an extremely useful resource to read next to this report when it comes to issues relating to personal data breach notifications.

# 3. Technical and organisational measures to ensure security

The majority of the decisions that relate to Article 32 GDPR focus on the LSA's assessment of the **appropriateness of the technical and organisational measures** to ensure a level of security appropriate to the risk. This issue is at the heart of a pending case before the Court of Justice of the European Union (CJEU)[9], which is actually the first case dealing

[3] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052, accessed 14.09.2023.

[4] EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, adopted on 14 December 2021 Version 2.0, p. 5, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en, accessed 14.09.2023.

[5] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted on 28 March 2023, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en, accessed 14.09.2023

[6] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted on 28 March 2023, p. 5, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en, accessed 14.09.2023

[7] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted on 28 March 2023, p. 5, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en, accessed 14.09.2023.

[8] EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted on 28 March 2023, p. 18, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en, accessed 14.09.2023

[9] CJEU, Pending Case, Natsionalna agentsia za prihodite (C-340/21).

with the interpretation of Article 32 GDPR. The referring court asked whether Articles 24[10] and 32 GDPR are to be interpreted as meaning that the occurrence of a personal data breach (by persons who are not employees of the controller and are not subject to its control) is sufficient to presume that the technical and organisational measures implemented are not appropriate. In case the answer to this question is negative, the referring court seeks guidance on the subject matter and scope of the judicial review of legality in the examination as to whether the technical and organisational measures implemented by the controller are appropriate pursuant to Article 32 GDPR.[11] Although the request for a preliminary ruling is made by a court in the context of national proceedings, the findings of the CJEU will be crucial for SAs as well.

While the CJEU has not issued its judgment yet, Advocate General Pitruzzella argued that it would seem illogical to assume that the intention of the EU legislator was to impose on the controller the obligation to prevent any personal data breach irrespective of the diligence in the preparation of security measures[12] and that the mere existence of a personal data breach is not in itself sufficient to conclude that the technical and organisational measures implemented by the controller were not 'appropriate' to ensure the protection of the data at issue.[13] The Advocate General highlighted that the assessment of the appropriateness of those measures must be based on a **balancing** exercise between, on the one hand, the interests of the data subjects, which generally tend towards a higher level of protection, and, on the other hand, the economic interests and technological capacity of the controller, which sometimes tend towards a lower level of protection. This balancing exercise must comply with the requirements of the general principle of proportionality.[14] The Advocate General confirmed that the appropriateness of the implemented security measures has to be assessed ***in concreto***, by verifying whether the specific measures were suitable to reasonably prevent the risk and minimise the negative effects of the breach.[15] Thus, according to the Advocate General, a court, or by analogy an LSA in the context of this present study, when performing its judicial review on legality must carry out a specific analysis of the content of security measures, the manner in which they were applied and their practical effects, on the basis of the evidence before it and the circumstances of the specific case.[16]

The decisions issued by SAs that deal with the appropriateness of technical and organisational security measures can be divided in three main categories and they will be analysed in this report following this categorisation: (a) personal data breaches due to malicious attacks by external entities (Section 3.1), (b) personal data breaches due to insufficient practices and systems of organisations (Section 3.2), and (c) personal data

[10] According to Article 24(1) GDPR, the controller is to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

[11] C-340/21, Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice, 2 June 2021.

[12] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 34.

[13] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 84.

[14] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 36.

[15] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 39.

[16] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 40.

breaches due to human error (Section 3.3). Each section is further divided into two sections, one on the preventive technical and organisations measures taken by the organisations and one on the remedial measures that were taken or should have been taken after the occurrence of a breach. Article 32 GDPR does not itself make an explicit distinction between "preventive" and "remedial" measures. Nevertheless, Article 33(5) GDPR provides that "the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article". In practice, SAs often made this distinction in their decisions when analysing the measures in place before and after a breach has occurred. The EDPB Guidelines 01/2021 on Examples regarding Personal Data Breach Notification also make this distinction when recommending, on the one hand, prior measures and, on the other hand, mitigating measures to put in place for specific use cases. Finally, a separate section is dedicated to the issues relating to passwords that spanned across all three aforementioned categories of personal data breaches (Section 3.4).

## 3.1 Personal data breaches due to malicious attacks by external entities

The majority of the cases decided under Article 60 GDPR concern malicious attacks carried out by external entities that led to personal data breaches. The LSAs' decisions already follow the approach suggested by Advocate General Pitruzzella, in the sense that the LSAs assess *in concreto* and on **a case-by-case basis** the technical and organisational security measures at stake. However, these is no common methodology used by all LSAs when assessing the relevant measures. As it will be illustrated below, the LSAs made some observations on the specific case, examined the types of personal data that were compromised by the data breach and examined whether the security measures were "sufficient" [e.g. EDPBI:DEBE:OSS:D:2020:103, EDPBI:DEBE:OSS:D:2021:293, EDPBI:DEBE:OSS:D:2021:222, EDPBI:DEBE:OSS:D:2022:349], "sensible" [EDPBI:DEBE:OSS:D:2019:75] or used similar terms. The LSAs examined the technical and organisational security measures that were already taken by the data controller (in the majority of the cases) or the data processor in order to decide whether there was a violation of Article 32 GDPR (Section 3.1.a). In some cases, the LSAs assessed the technical and organisational security measures taken by the data controller (or the data processor) after the occurrence of a personal data breach or recommended appropriate measures that should be taken in order to prevent such a breach (Section 3.1.b).

### a. Preventive technical and organisational measures

In cases of malicious attacks, the LSAs looked both at the organisational, as well as the technical measures already taken by the company before the occurrence of the personal data breach. They also sometimes provided guidance to the companies on the measures they should take to avoid such breaches in the future.

One LSA adopted a decision with respect to the responsibility of a data controller for the technical and organisational measures that were already taken by a previous company it acquired. Before the **acquisition of the company**, the attacker installed Remote Access Trojans (RATs) but only ran an attack at a later point in time, when the company was already purchased by a new data controller, which resulted in a personal data breach. The data controller was not aware of the already installed infiltrating web shell at the time of the acquisition. Nevertheless, the LSA found that the data controller failed to process personal data in a manner that protects them against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 32 GDPR [EDPBI:UK:OSS:D:2020:155], highlighting the responsibility of the data controller for taking such measures.

As regards **organisational measures**, LSAs paid special attention to the existence of company policies relating to data security, such as an established strict policy against phishing (which included policy for passwords, internet usage and personal devices) and frequent awareness-raising campaigns for employees [EDPBI:ES:OSS:D:2022:382]. An SA also analysed the established practice of a company that reminded and continuously informed the employees about the safe handling of emails [EDPBI:DK:OSS:D:2021:288].

All decisions that relate to personal data breaches caused by malicious attacks examined thoroughly the **technical measures** put in place by the company before the occurrence of the security incident. One LSA clarified that the risk should not be assessed only at the time of the implementation of a technical measure, but "given the technological evolution of personal data processing activities [of the data controller], [it] must be addressed from the point of view of **continuous risk management**, by defining the control and security measures that are necessary to ensure that the processing takes place in compliance with the privacy and confidentiality of the data and by regularly and continuously assessing the effectiveness of the control measures put in place" [EDPBI:ES:OSS:D:2021:239].

Further, another LSA found that the requirement under Article 32 GDPR on adequate security normally implies that in systems with a large number of confidential information about a large number of users, **higher requirements** must be imposed on the controller when ensuring that there is no unauthorised access to personal data. This LSA specified that all likely outcomes should be tested in the context of the development of software where personal data are processed, as it noted that Article 32(1)(d) GDPR specifically mentions "a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security of the processing" [EDPBI:DK:OSS:D:2022:380]. In one case, the LSA found that the mechanism used by the company to encrypt the bank details[17] presented vulnerabilities. According to this LSA,

[17] In particular, determination in advance of the vector initialisation, reuse of it and obsolescence of the library used.

this does not, in view of the sensitivity of this data, ensure a level of security appropriate to the risk and constitutes a violation of Article 32 GDPR. The LSA recommended the implementation of increased security measures, such as encryption of sensitive data [EDPBI:FR:OSS:D:2023:802].

The **encryption** of personal data has been at the centre of various LSAs' decisions on security. In one case, the attacker exploited a security vulnerability but the data controller had already in place HTTPS encryption, two-factor authentication, and password hashing (bcrypt). The LSA did not attribute any negligence to the data controller since the security vulnerability occurred in the latest version of a third-party software [EDPBI:DEBE:OSS:D:2021:211]. Conversely, in a case where the data controller used the HTTPS protocol for its websites, but not on pages with contact forms through which information such as the name, the e-mail address and any free text was submitted by individuals to the company, the LSA found that this lack of encryption constituted a violation of Article 32 GDPR [EDPBI:SE:OSS:D:2021:300]. In another case, the implementation of the HTTP protocol instead of HTTPS when accessing a website, including the page for collecting bank account data, was considered an insufficient security measure, leading to a breach of Article 32 GDPR. [EDPBI:FR:OSS:D:2023:802]. The LSA made a reference to the recommendation of ANSSI, the French National Information Security Agency, that the implementation of **HTTPS** on a website or a web application is a security safeguard to ensure the confidentiality and integrity of the information exchanged, as well as the authenticity of the server contacted, concluding that the absence of this safeguard can lead to many abuses without malicious intent[18] [EDPBI:FR:OSS:D:2023:802].

In a case where all requests were sent to the server by an application and a smart watch in a non-secure "**http**" format, the LSA recommended that the data controller should encrypt the channel used for all requests [EDPBI:FR:OSS:D:2021:186]. Several cases, dealt with the technical measures taken for email encryption, or the lack thereof. In one case, the data controller had sent sensitive data regarding health to a data subject via email, which was encrypted with so-called Enforced Transport Layer Encryption (Enforced TLS-encryption), encrypting the message from the e-mail servers of the data controller to the recipient's e-mail server. The LSA found that the data controller only encrypted the e-mail during the transport. This implied that the encryption ended before the message had reached the final recipient and, thus, did not constitute an **end-to-end encryption**. In the period following the complaint, the data controller developed and launched a new communication solution for e-mails sent to its customers, who would get access to their emails via the "My Pages" section on the data controller's website. Such system required authentication using the national e-identification system. The LSA found these new

[18] ANSSI (Agence Nationale de la Sécurité des Systèmes d' Information), Recommandations pour la mise en œuvre d'un site web: Maîtriser les standards de sécurité côté navigateur, 2021, available online at https://www.ssi.gouv.fr/uploads/2013/05/anssi-guide-recommandations_mise_en_oeuvre_site_web_maitriser_standards_securite_cote_navigateur-v2.0.pdf (only in French).

security measures appropriate when assessing the responsibility of the data controller for the data breach [EDPBI:SE:OSS:D:2023:652].

The use of outdated OpenVPN server version and open SSH ports has been considered security vulnerabilities that can lead to security incidents [EDPBI:DEBE:OSS:D:2020:114]. In another case the data controller had activated TLS encryption for the most common recipient mail servers; however the LSA found that the lack of use of TLS encryption for communication to other less common recipient servers constitutes a failure to comply with the data controller's security and confidentiality obligations under Article 32 GDPR and made a reference to the ANSSI Security Recommendations for TLS[19] [EDPBI:FR:OSS:D:2021:307].

The **unencrypted storage** of data at the time of malicious attacks reveals a lack of technical measures to protect the data. The existence of a backup copy of a database stored in the controller's online storage without encryption, which resulted in a personal data breach, was found to lead to a violation of the company's Article 32 GDPR obligations [EDPBI:LT:OSS:D:2021:298].

SAs required companies to retain **log records** that save when specific (sets of) data were accessed, and by whom [EDPBI:LT:OSS:D:2021:298]. One LSA clearly declared that the establishment of activity logs, i.e. the recording of activities in "log files" or "logs", particularly for access to the various servers of an information system, is crucial in that it enables the activities to be traced and it allows to detect any anomalies or events related to security, such as fraudulent access and misuse of personal data. The LSA made a reference to the ANSSI Security recommendations for logging system architecture, which highlight the importance of and the necessity for recording event logs[20] [EDPBI:FR:OSS:D:2021:313]. Similarly, the lack of review of any logging code was found to lead to a violation of Article 32 GDPR [EDPBI:UK:OSS:D:2020:147]. Although not mentioned in any decision, it is useful to add that the logging of events linked to administration accounts was also highlighted in the ANSSI Recommendations to secure administration of IT systems.[21] With regard to the review of logging codes, a reference was further made to the OWASP guidance on code review, which suggested that a review of any logging code should be performed to identify, amongst other things, what

[19] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Security Recommendations for TLS, Last updated in 2017, available at https://www.ssi.gouv.fr/guide/security-recommendations-for-tls/. The latest version of the recommendations are only available in French, ANSSI, Recommandations de sécurité relatives à TLS, 2022, available at https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/ (in French).

[20] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Recommandations de sécurité pour l'architecture d'un système de journalisation, 2022, available at https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/ (only in French).

[21] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Recommendations to secure administration of IT systems, 2018, available at https://www.ssi.gouv.fr/guide/secure-admin-is/. A more recent version of these recommmendations is only available in French: ANSSI, Recommandations relatives à l'administration sécurisée des systems d'information, 2021, https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/ (in French).

information should not be logged, such as sensitive personal data and some forms of personally identifiable information[22].

Next to this requirement, the LSAs examined the establishment of proper **access control mechanisms** that can be ensured via the individual authentication of persons that are allowed to access specific (sets of) data. The lack of such clear access control mechanisms led to violations of Article 32 GDPR [EDPBI:FR:OSS:D:2019:73; EDPBI:LT:OSS:D:2021:298; EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310; EDPBI:DK:OSS:D:2021:282; EDPBI:FR:OSS:D:2021:186]. In some of these cases, one LSA made a reference to the ANSSI recommendation to use by default individual administration accounts.[23]

In one case, the LSA directed the data controller to several sources that contain recommendations for effective and suitable countermeasures that help prevent the compromising of an internet platform (such as a web shop) through the infiltration and execution of malware. Indicatively the LSA referred[24] to:

the IT-Grundschutz-Compendium of the German Federal Office for Information Security[25]: With regard to web applications and web services, there are a number of countermeasures discussed, including for example the mandatory controlled *integration of files and content* (APP.3.1.A.4) or the recommended *penetration testing and auditing* (APP.3.1.A22).

the Guideline "State of the Art" published by the IT Security Association Germany (TeleTrust)[26]: With regard to web applications or web service interfaces, they mention measures to be used against IT security threats, such as command injection, the use of a *Web Application Firewall* (WAF or WSF) that analyses communication and blocks potentially harmful data traffic, among others; and

the documents of the Open Web Application Security Project (OWASP)[27]: which list "injection" as a significant security risk and recommend input validation as a countermeasure. In addition, the test for uploading malicious files is part of the Web

[22] OWASP (The Open Source Foundation for Application Security), OWASP Code Review Guide, 2017, available at https://owasp.org/www-project-code-review-guide/.

[23] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Recommendations to secure administration of IT systems, 2018, available at https://www.ssi.gouv.fr/guide/secure-admin-is/. A more recent version of these recommmendations in only available in French: ANSSI, Recommandations relatives à l'administration sécurisée des systems d'information, 2021, https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/ (in French).

[24] The references have been updated to the provisions that are currently applicable.

[25] Bundesamt für Sicherheit in der Informationstechnik-BSI (Federal Office for Information Security), IT-Grundschutz-Compendium, last updated on 1 February 2022, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2.

[26] The Guideline has been updated and the latest version is: IT Security Association Germany (Teletrust) in cooperation with ENISA, Guideline "State of the Art", 2023, available at https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/?tx_reintdownloadmanager_reintdlm%5Bdownloaduid%5D=11374&cHash=c54bc0d66a24eaf47777f8986f37d997.

[27] see https://www.owasp.org.

Security Testing Guide of the OWASP (point 4.10.9)[28], and should therefore be carried out regularly before commissioning and during operations when testing web applications [EDPBI:DEBB:OSS:D:2021:308].

## b. Remedial technical and organisational measures

When deciding on cases where data breaches occurred due to malicious attacks, the LSAs assessed in detail the technical and organisational measures that organisations took after the data breach.

In some complex cases, the LSAs examined all measures, both technical and organisational, taken by a company as a whole in order to assess whether these would be deemed appropriate in light of Article 32 GDPR. The LSAs did not indicate whether all these measures should be taken cumulatively or some of them are more important than others to satisfy the obligations arising from Article 32 GDPR. In one such case, the LSA found that a company took satisfactory and appropriate technical and organisational measures after a **ransomware** attack: the data controller closed their servers, isolated the systems to contain the cyber-attack and ordered a forensic analysis of the incident. Technical measures were also taken at a network level, such as the retrieval and security of the servers concerned or the activation of existing backups. In the context of the forensic analysis, constant real-time monitoring was carried out, including the analysis of access records (logs), system analysis and network traffic analysis. In addition, senior management, legal and IT teams were also involved in the incident analysis to create contingency plans and take appropriate measures in each business unit. Finally, after the data breach, a number of measures were taken by the affected company in order to strengthen its security measures and to be able to monitor its efficiency, including the hiring of an external security company to carry out a specific audit of the security elements of the group, procurement of IT tools and their monitoring by certified partners, review and updating of security measures[29]. Analysing these measures, the LSA found that there was no evidence to indicate a lack of diligence or inadequate measures after the incident, without however stating that the measures were appropriate [EDPBI:ES:OSS:D:2022:382]. In contrast, in another case where the data controller took a number of technical and organisational measures following a malicious attack[30], the LSA issued a reprimand [EDPBI:EE:OSS:D:2021:289].

[28] OWASP, Web Security Testing Guide, v4.2, 2020, available at https://owasp.org/www-project-web-security-testing-guide/.

[29] Such measures included the strengthening of access control, increasing the complexity of passwords and shortening the renewal period, carrying out sessions analysis on a more regular basis, installing a general prohibition of the use of personal devices (only allowed in exceptional cases), monitoring the use of unauthorised applications, allowing the use of authorised file sharing tools only, reinforcing recommendations on sending sensitive information (personal data, confidential data, etc.) in encrypted attachments.

[30] The measures included the following: the data controller 1) prepared a plan to train employees in the field of information security; 2) mapped the scope of the incident and identified a system that enabled

Several measures taken by a data controller following a data breach were found not appropriate in light of Article 32 GDPR. These included the exchange of **SSH keys** for authorised access, the monitoring of relevant system files for changes in access keys, the checking of the system's open ports, as well as of all system and home directories for malware and unwanted files and deleting them if necessary, and blocking the execution of PHP scripts from certain directories [EDPBI:DEBB:OSS:D:2021:308].

Conversely, in a similar case, the data controller immediately isolated the entire infected server and took it offline, as soon as they became aware of the data breach. New internal system passwords were also assigned. The data controller stored the affected server for investigation and prosecution purposes in the same condition as the attacker left it. The data controller further reverse-engineered the attack script. The attacker's attempts to penetrate even deeper into the systems and onto other servers of the data controller were prevented by further security measures already in place at the time (including IP restrictions). The LSA found these measures appropriate [EDPBI:DEBE:OSS:D:2021:211].

The switch to a more **secure cloud service** was recognised by an LSA as an enhanced security measure [EDPBI:DEBE:OSS:D:2020:99].

Following data breaches that occurred via compromised employee profiles or employee hardware, the LSAs welcomed measures that led to the isolation of the **compromised profile or hardware**. In one case, the compromised profile of the employee of the controller as well as their personal computer were localized and were temporarily deactivated. Further, the employee's access to all shared private spaces and partner platforms was blocked. Any outside access to the system on the part of employees was restricted. All the information stored on the hard disk of the compromised personal computer was deleted and reinstalled. The employee of the controller whose personal computer had been compromised was provided with a new wireless internet router to enhance security [EDPBI:BG:OSS:D:2023:659].

Following a cyberattack where the attackers had obtained the names and passwords of customer accounts, the data controller blocked access and reset passwords, recommending affected customers via email to change their passwords. The data controller also installed a new patch to block suspicious IP addresses after a failed authentication attempt. The LSA found these steps appropriate to minimise the risk and to eliminate the adverse consequences of the data breach [EDPBI:AT:OSS:D:2021:264].

unauthorized processing of personal data by third parties; 3) informed the data subjects affected by the violation; 4) checked the logs of the databases of their systems, including the access logs of the employees, and engaged a third party vendor that specialises in information security, to help improve the situation; 5) initiated a project to transfer customer data to a database subject to even stricter security requirements; 6) performed regular stress tests on existing as well as new systems; 7) reviewed the restrictions on access to all databases and limited the number of users who can access sensitive customer information; 8) audited the users of the customer management software; 9) audited all user accounts that have access to the customer data database; 10) prepared instructions for customer support / sales department on how to help and what data to collect from persons who turn to [blanked out name] for a given data breach; 11) implemented a comprehensive security solution, which helps to prevent the occurrence of similar incidents in the future; 12) checked the security of the mobile app; 13) performed compliance control of information security standards and requirements; and 14) has been able to stop the leakage by taking appropriate measures.

In several cases where the credentials providing access to systems of the data controller or to user profiles were compromised, the LSAs welcomed the subsequent installation of **two/multi-factor authentication** [EDPBI:DEBE:OSS:D:2020:133; EDPBI:BG:OSS:D:2023:659; EDPBI:DEBE:OSS:D:2019:75; EDPBI:DEBE:OSS:D:2020:124; EDPBI:DEBE:OSS:D:2020:125]. When the companies did not introduce such measures, the LSAs recommended in several cases the use of two/multi-factor authentication as a security measure to ensure stronger authentication [EDPBI:DEBE:OSS:D:2020:136, EDPBI:DEBE:OSS:D:2022:468; EDPBI:HU:OSS:D:2020:116; EDPBI:UK:OSS:D:2020:147].

In another case, the LSA recommended that the data controller should implement a system ensuring authentication of requests between the application and the sever (by means of a TLS protocol, for example) so that the server only accepts requests coming from known users with a right of access [EDPBI:FR:OSS:D:2021:186].

Transparency measures towards data subjects affected by the data breach, even when a notification is not mandatory in accordance with Article 34 GDPR, are welcome by LSAs. LSAs positively consider cases where data subjects are informed of the breach and warned whenever relevant to be vigilant about any future messages sent to them [EDPBI:BG:OSS:D:2023:659; EDPBI:EE:OSS:D:2021:289].

Following data breaches, data controllers also introduced an email notification system to inform users about an unauthorised access attempt, and push notifications to the mobile device linked to the relevant user profile [EDPBI:BG:OSS:D:2023:659].

The strengthening of **access control** to authorisation databases, by limiting the number of employees who have access to it and who have personalised accounts, was found to be a satisfactory measure taken by a data controller following a data breach [EDPBI:DEBE:OSS:D:2020:124].

Following personal data breaches, companies established a new internal policy and a new procedure for security enhancement, which were considered by the LSA to be appropriate **organisational measures** to address future attacks [EDPBI:BG:OSS:D:2023:659].

After the occurrence of personal data breaches, LSAs considered to be a satisfactory organisational measure the delivery of internal training to employees in order to raise their awareness of cyber security and the security of personal data processing [EDPBI:BG:OSS:D:2023:659; EDPBI:EE:OSS:D:2021:289].

## 3.2 Personal data breaches due to insufficient company practices and systems

Often data breaches occur due to insufficient company practices and systems. The LSAs firstly examine the technical and organisational measures already taken by the company in order to ensure a level of security appropriate to the risk, and if these are found not to be appropriate. Secondly, LSAs examine the possible measures taken by the company after the occurrence of the data breach and in some cases propose measures that would be considered appropriate in this context to prevent such data breaches from taking place in the future. As company practices and systems can be very specific relating to the data breach in question, the measures discussed in this section are once again examined *in concreto* and are tailored to each specific data breach. Nevertheless, there is great value in creating an understanding of what measures the LSAs consider appropriate in relation to specific data breaches and what not in this context. It shall be clarified that SAs' decisions that relate to data breaches stemming from hacking are covered above in Section 3.1, even if the attacked organisations also had insufficient security practices and systems.

### a. Preventive technical and organisational measures

The first step that all SAs take when deciding on a case where data breaches have taken place is to examine what technical and organisational measures the company had already implemented before the occurrence of the data breach and to assess whether these were appropriate to ensure a level of security appropriate to the risk.

Often the implementation of security measures is outsourced to data processors. In that regard, one LSA found that the breach of personal data suffered by one company was caused in particular by a lack of vigilance by the controller regarding the measures implemented by its **data processor** responsible for securing its website. The LSA clarified that controllers are required to continue to monitor regularly the effectiveness of the technical and organisational measures implemented to ensure the security of the processing, including the effectiveness of the measures taken by their processor [EDPBI:FR:OSS:D:2021:181].

The way in which information is provided to the company's customers was at the centre of several cases on which LSAs decided. The practice of sending encrypted and **password protected documents** to company users via a first email, followed by a second email shortly after, with the corresponding (very weak) passwords in an email that was only transport-encrypted was found not "sufficient" within the meaning of Article 32 GDPR [EDPBI:DEBB:OSS:D:2020:139]. Similarly, the practice of sending personal data to data subjects in response to personal data access requests via two separate emails was found to violate Article 32 GDPR obligations. More specifically in this case, one email was sent with a data extract in CSV format, in the form of an encrypted archive, and the second email contained the password to the archive [EDPBI:FR:OSS:D:2021:202]. Concrete recommendations from the LSAs on the sending of passwords can be found in section 3.4.

One LSA considered that a controller that had a manual system to deny suspicious high-frequency login trials (as opposed to an automatic one) had not put in place "adequate" organisational and technical measures to ensure a level of security appropriate to the risks involved in the processing of personal data [EDPBI:DK:OSS:D:2021:207].

A company practice enabling a computer used by one of the database's administrators to connect to the management tool without going into "sleep" mode was found by the LSA to be in breach of Article 32 GDPR. In fact, the user's session was never automatically locked after a prolonged period of inactivity, e.g. after the employee leaves his workstation, and third parties could therefore access the data processed on said computer [EDPBI:FR:OSS:D:2019:73].

Company practices relating to the processing of bank card information were also assessed by LSAs. One LSA found that the measures put in place by a company that enabled customers to send photographs or scans of their bank cards containing all bank card numbers in clear text by **unencrypted email** from their mailbox were in breach of Article 32 GDPR. In this case, such data were stored, as was the documentary proof requested for the purposes of combatting fraud, for six months in clear text in the database of the controller [EDPBI:FR:OSS:D:2020:134].

Security of processing of personal data was also one of the issues examined in a complex case on online advertising. A European-level association for the digital marketing and advertising ecosystem developed a Transparency and Consent Framework (TCF), which is a standard to facilitate the digital advertising industry's compliance with certain EU privacy and data protection rules. Specifically, under the TCF, some companies offer "Consent Management Platforms" (CMPs), which are pop-up windows that record user preferences to online trackers (such as cookies), that is to say whether users consent to cookies or not. An essential part of the CMP is the generation of a character string consisting of a combination of letters, numbers and other characters, called "Transparency and Consent String" (TC String). The TC String is meant to capture in a structured and automated way the tracking preferences of a user when he or she visits a website or app of a publisher that has integrated the CMP. Privacy organisations argued in their complaint that the integrity of the TC String was not sufficiently ensured, since it was possible for the CMPs to falsify the signal and thus reproduce a "false consent" of the users for the different trackers. The LSA argued that the security and integrity obligations do not only entail organisational but also technically effective measures to ensure and demonstrate the integrity of the consent signal transmitted by CMPs to adtech vendors [EDPBI:BE:OSS:D:2022:325]. This decision led to the request for a CJEU preliminary ruling by the Brussels Court of Appeals (Hof van beroep te Brussel).[31]

## b. Remedial technical and organisational measures

Following a data breach and after assessing the companies' practices and systems, LSAs assessed the technical and organisational measures that companies eventually took as a

[31] Pending Case, IAB Europe (C-604/22).

response to the breach and made recommendations for (further) measures in order to prevent such data breaches in the future.

On the practice of sending personal data to data subjects in response to personal data access requests via two separate emails[32], the LSA ordered the data controller to use different channels for sending personal data in the form of encrypted archives and the password, possibly by sending the password by SMS when the encrypted archive is sent by email [EDPBI:FR:OSS:D:2021:202].

A data controller used a tool that would generate URLs when documents were sent by the company's users via email. Although the data controller modified the tool configuration so that it would send to the customers the relevant documents as attachments to a confirmation email, it was unable to delete the links that had previously been created. The LSA found a breach of the security obligations of the data controller. It ordered the data controller to make all supporting documents still retained in the form of links in the tool inaccessible to third parties without prior authentication, possibly by having them communicated in the form of attachments, as has been done for supporting documents sent following the configuration modification [EDPBI:FR:OSS:D:2021:202].

One LSA found that using fictitious or anonymised data in the context of **IT testing** constitutes an essential security precaution to adopt for IT developments. The LSA found a violation of Article 32 GDPR and ordered the data controller to cease using actual personal data for the development and testing phases [EDPBI:FR:OSS:D:2021:306].

In the case of the Transparency and Consent Framework (TCF) (see above section 3.2.a), the LSA ordered to adopt effective technical and organisational monitoring measures to guarantee the integrity of the TC String in view of the possibility of falsification of the signal, such as a strict vetting process for organisations participating in the TCF. The LSA also ordered strict audits of organisations that join the TCF to be carried out in order to ensure that participating organisations meet the requirements of the GDPR, including security of processing [EDPBI:BE:OSS:D:2022:325].

## 3.3 Personal data breaches due to human error

Undoubtedly, since technical systems often involve the intervention of natural persons, such as employees of the company or end users, sometimes data breaches occur due to human errors. Similar to the two previous sections, LSAs firstly examine the technical and organisational measures already taken by the company in order to ensure a level of security appropriate to the risk preventing the possibility for human error. Secondly, and if these are found not to be appropriate, LSAs examine the possible measures taken by the company after the occurrence of the data breach and in some cases propose measures that would be considered appropriate in this context to prevent such data breaches from taking place in the future. Security measures to adopt in the context of

[32] See previous section for details on the case EDPBI:FR:OSS:D:2021:202.

data breaches occurring as a result of human error are also case-specific and the assessment of the LSAs is done on a case-by-case basis. However, important lessons can be drawn on what measures the LSAs consider appropriate in relation to specific data breaches and what not in this context.

## a. Preventive technical and organisational measures

Data breaches resulting from human error often relate to the **disclosure of email addresses** via email. The sending of mass emails where all recipients were in copy has been found to constitute an infringement of the data security obligations of the data controller. The LSAs found a lack of appropriate technical and organisational measures to prevent the data breach [EDPBI:CY:OSS:D:2021:182; EDPBI:FR:OSS:D:2021:169].

One LSA found that the **accidental** disclosure of personal data of one customer to another customer constituted an infringement of the data controller's obligations under Article 32 GDPR. However, the fact that the data controller had adopted a mandatory internal procedure for reporting and notifying personal data breaches was considered a mitigating circumstance. This internal procedure comprised of individual steps to be taken after becoming aware of a breach, such as handling the incident, documenting the incident and taking corrective measures. This procedure also included a method to carry out a risk assessment and notification of a breach [EDPBI:CZ:OSS:D:2019:44].

The lack of sufficient **testing of solutions** created to enhance the security of personal data within a system, allowing vulnerabilities that led to a data breach, was found to be in violation of Article 32 GDPR [EDPBI:IS:OSS:D:2021:216].

## b. Remedial technical and organisational measures

Following a data breach resulting from the disclosure of email addresses of candidates to **all the email recipients**, the data controller proposed as a corrective measure to require employees to obtain the prior approval of a Director and the DPO before any external email could be sent to more than three data subjects. The data controller also suggested that the employee who made the error would be subject to a disciplinary hearing and would have to undertake further training. However, the LSA did not consider these measures appropriate to meet the requirements of Article 32 GDPR and required additional technical measures to be implemented by the data controller to prevent such an incident from occurring in the future. More concretely, the LSA required an alert message to be clearly displayed every time an email is sent to recipients outside the organisations and to disable the 'cc' field or limit the number of email addresses that this field can contain. In addition, the LSA required that whenever a mass email is to be sent, an information message pops-up on the sender's screen in a manner that cannot be missed and, ideally, preventing the user from sending the email unless a positive action is taken, such as prompting the user to close the pop-up. The LSA also required the company to set up rule to delay the delivery of any email message [EDPBI:CY:OSS:D:2021:182].

In a case where breaches took place due to human errors when assigning employees of a company **access rights** to employees' data, the LSA acknowledged the mitigating circumstance that the data controller had taken measures to ensure the restriction of access. These measures included, inter alia, the development of new time registration systems, the development of procedures for continuous control of employees' access rights in the form of posting lists of job roles for review, and the organisation of internal as well as external audits [EDPBI:DK:OSS:D:2021:190]

The offering of **data protection training** by the data controller following a data breach due to human error was considered a sufficient security measure in several cases [EDPBI:DEBE:OSS:D:2020:103; EDPBI:DEBE:OSS:D:2021:197].

Following a data breach caused by a faulty configuration of the development environment by an employee, the LSA considered the immediate revocation of the token in question a sufficient security measure [EDPBI:DEBE:OSS:D:2020:103].

In one case that led an **unencrypted backup** of a database to become publicly accessible due to a human error, the LSA considered the mitigating measures taken by the data controller as a whole as sufficient. The mitigating measures included the actual deletion of the compromised backup, the blocking of the affected data storage, the provision of written information to employees on the necessary security precautions when handling personal data and the change of all passwords and access codes to the company's own systems and integrated third-party systems [EDPBI:DEBE:OSS:D:2021:187].

Following a breach of personal data relating to a customer, the data controller blocked the compromised customer account, changed the accessed data, organised data protection training for employees and the company's DPO carried out a data protection audit. The LSA considered these measures sufficient [EDPBI:DEBE:OSS:D:2021:197].

In several cases where non-critical personal data (often names, email addresses or telephone numbers) became publicly available, the LSA found that the prompt removal of the faulty code or erasure of the data by the data controller was  a sufficient measure [EDPBI:DEBE:OSS:D:2021:293, EDPBI:DEBE:OSS:D:2021:222, EDPBI:DEBE:OSS:D:2022:349].

## 3.4Passwords as preventive technical and organisational measure

Several LSAs analysed the issue of security of passwords in the context of Article 32 GDPR, as a necessary measure to ensure security of personal data.

### Passwords complexity & transmission

In a case where a company generated very simple passwords ("first name last name123") for its customers, the LSA highlighted that the password itself must be **state-of-the-art**. In particular, the password must be sufficiently complex to be difficult to guess. The LSA highlighted that the German Federal Office for Information Security has provided guidance on the appropriate measures to adopt for the creation and transmission of passwords in the IT-Grundschutz-Compendium [EDPBI:DEBB:OSS:D:2020:139].

The IT-Grundschutz-Compendium as last updated in February 2022[33] contains concrete rules on the creation and transmission on passwords in module "CON.1 Crypto Concept" and "ORP.4: Identity and Access Management". The 2022 Compendium contains in particular provisions governing the use of passwords (ORP.4.A8), rules on the regulation of password quality (ORP.4.A22) and on the regulation of password-processing applications and IT systems (ORP.4.A.23)[34].

The issue of password encryption when sharing the password with users was dealt with in several decisions. One LSA recommended that the data controller would no longer send passwords **in clear text by email**, especially during the creation of a user account [EDPBI:FR:OSS:D:2019:73].

The **complexity** of passwords has been thoroughly examined in several decisions in order to assess whether the rules put in place by companies meet the requirements established in Article 32 GDPR. A seven-character password containing only lowercase and uppercase letters was found by one LSA to be in breach of the obligation to ensure the security of data, also due the fact that the password was sent by the data controller to the user by email in clear text [EDPBI:FR:OSS:D:2019:73]. Similarly, practices that allowed simple passwords to be created did not meet applicable requirements in terms of strength and the LSA gave recommendations on what constitutes a secure password[35] [EDPBI:FR:OSS:D:2020:134; EDPBI:FR:OSS:D:2020:193; EDPBI:FR:OSS:D:2021:181; EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310; EDPBI:FR:OSS:D:2023:802].

One LSA found that the passwords accepted by the data controller were not robust. The LSA also noted that there was no implemented renewal policy for passwords. It further observed that the password hashing MD5 algorithm that used in the database and the password modification URL were obsolete in terms of security, insofar as it had widely known vulnerabilities that made it easily reversible in the event of passwords being disclosed in their hashed form. Thus, the LSA ordered the data controller to implement a binding policy on passwords, in particular in terms of complexity, providing for the

[33] Bundesamt für Sicherheit in der Informationstechnik-BSI (Federal Office for Information Security), IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd Edition 2020. The Compendium was last updated on 1 February 2022, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2.

[34] Bundesamt für Sicherheit in der Informationstechnik-BSI (Federal Office for Information Security), IT-Grundschutz-Kompendium, 1 February 2022, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2, under ORP.4 Identity and Access Management: Section 3.1.

[35] See below in Section 3.4/ FR SA recommendation: "Passwords: a new recommendation for controlling your security".

renewal of passwords (every six months, for example). This decision is interesting because the LSA referred to a recommendation of the CNIL ("FR SA")[36] on what would constitute a robust password [EDPBI:FR:OSS:D:2021:186]. Similar reflections on what constitutes a strong password have been made in other decisions as well, which refer to the 2017 FR SA recommendation or to the content of it, such as in EDPBI:FR:OSS:D:2021:306. This recommendation of the FR SA was updated through a new recommendation adopted in October 2022 and is worth presenting due to its comprehensiveness and completeness.[37]

### *FR SA's recommendations: "Passwords: a new recommendation for controlling your security"*

According to the FR SA, means of authentication such as two-factor authentication or electronic certificates offer more security than passwords. The FR SA also referred to the ANSSI recommendations on multi factor authentication and passwords[38]. The new FR SA recommendations emphasised the degree of complexity that the password must have (entropy) and rather than a minimum length, in order to offer more freedom in the definition of robust password policies adapted to different use cases. More concretely, the FR SA defines a generic minimum level of 80 bits of entropy for a password without additional measures, and leaves organisations free to define their password policy. The recommendations contain three examples that are equivalent in terms of entropy and all meet the requirements of the new recommendation:

**Example 1**: passwords must be composed of at least 12 characters including uppercase letters, lowercase letters, numbers and special characters to choose from a list of at least 37 possible special characters.

**Example 2**: Passwords must be composed of at least 14 characters including uppercase letters, lowercase letters and numbers, without mandatory special characters.

**Example 3**: a passphrase must be used and it must be composed of at least 7 words.

The new FR SA's recommendations further abandoned the obligation to renew passwords for standard user accounts. In that regard, renewal remains required only for "privileged" accounts, i.e. administrator type or with extended rights. The

[36] Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033928007

[37] CNIL (Commission Nationale de l'Informatique et des Libertés), Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, 14 October 2022, available at https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite (only in French).

[38] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Recommandations relatives à l'authentification multifacteur et aux mots de passe, 08 October 2021, available at https://www-ssi-gouv-fr.translate.goog/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp (only in French).

recommendations also offered clarification on the rules concerning the creation and renewal of passwords to guarantee a constant level of security throughout the life cycle of the password in the form of good practices (password manager, non-use of obvious information).

In its new recommendations, the FR SA identified three cases of password identification, which are associated with different entropy levels: a) simple password authentication, b) passwords with access restriction mechanisms (such as account access delay after several failures; maximum number of attempts allowed within a given time frame, "Captcha", etc.) and c) passwords for hardware unlock code (with equipment owned by the user, e.g. SIM card, bank card etc., complemented with account blocking after three failed attempts).

The FR SA highlighted that passwords should never be stored in plain text and recommended that when authentication takes place on a remote server, and in other cases if technically feasible, the password must be transformed using a non-reversible and secure cryptographic function, incorporating the use of a salt or of a key, such as scrypt or Argon2.[39]

### *Storage of passwords*

In several decisions, the LSAs had the opportunity to reflect on the issue of the storage of passwords, requiring strong encryption for the stored passwords.

In one case, the data controller had saved passwords in plain text, as part of scripts to arguably 'aid functionality' and did not require employees to enter passwords upon the execution of script(s). The LSA found that the storage of passwords in plain text was not acceptable, in violation of Article 32 GDPR [EDPBI:UK:OSS:D:2020:147].

One LSA found that the **hashing of passwords** with PBKDF2-SHA 256 using salt values was a satisfactory technical measure taken by the data controller to prevent the disclosure of the passwords on a large scale [EDPBI:DEBE:OSS:D:2020:124]. Another LSA found that implementing a satisfactory hashing system of passwords, using SHA256 [EDPBI:FR:OSS:D:2021:279] or BCRYPT [EDPBI:FR:OSS:D:2021:310] was an appropriate technical measure to meet the Article 32 GDPR obligations.

Another LSA found that the authentication of employees to the databases was insufficiently secure because the passwords were stored, unencrypted, in a text file located on a company computer. This LSA therefore found a violation of Article 32 GDPR [EDPBI:FR:OSS:D:2021:279]. In one case, the data controller was using the Bcrypt algorithm for the storage of platform users' passwords, but the account passwords created before 2013 were retained in a database in hashed format, using SHA1 algorithm

[39] CNIL (Commission Nationale Informatique & Libertés), Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, 14 October 2022, available at https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite (only in French).

with salt. The LSA found that the SHA1 hashing function has known vulnerabilities that make it impossible to guarantee integrity and confidentiality of passwords in the event of a brute force attack after the servers hosting them have been compromised. The LSA found a violation of Article 32 GDPR and required the data controller to replace the SHA1 hashing algorithm with salt by an algorithm acknowledged to be strong, possibly by obliging users to delete their current passwords [EDPBI:FR:OSS:D:2021:202]. SHA1 has been found to be a weak and unsafe password encryption method in other cases, resulting in a breach of Article 32 GDPR [EDPBI:LT:OSS:D:2021:298; EDPBI:FR:OSS:D:2020:193].

In another case, the data controller had set up a password hash for the user accounts of the website using the MD5 + salt algorithm. However, the LSA recommended using hashing algorithms deemed strong for the storage of password and ordered the use of a recognised and secure algorithm, such as tor example bcrypt, scrypt or PBKDF2 [EDPBI:FR:OSS:D:2021:306]. In several cases, the LSA found that using MD5 hash function for the storage of passwords was obsolete, was not considered state-of-the art and did not guarantee the security of the data within the meaning of Article 32 GDPR [EDPBI:FR:OSS:D:2021:186; EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310].

# 4. Notification and/or communication of personal data breaches

The notification of personal data breaches to the Supervisory Authority, as well as the communication of personal data breaches to the data subjects do not seem to raise significant concerns in Decisions taken under Article 60 GDPR.

## 4.1Notification of personal data breaches to the Supervisory Authority

In one decision, the LSA established that the data controller was aware of a data breach but failed to notify the relevant supervisory authority. Interesting in the specific decision was that the LSA focused on the interpretation of the obligations for data controllers under Article 33(5) GDPR regarding the **documentation** of the data breach. The LSA concluded that the documentation provided by the data controller did not contain sufficient information to allow the LSA to verify the compliance of the data controller with the requirements of Article 33 GDPR, as it was rather documentation of a general nature, including reports and internal communications, that were generated in the context of the management of the incident by the data controller. The LSA found a violation of Articles 33(1) and 33(5) GDPR [EDPBI:IE:OSS:D:2020:165]. In another case, the data controller did not notify the LSA of a personal data breach within the time period established in Article 33(1) GDPR. The data controller contended that they were preparing a meaningful notification combining several similar data breaches. However, the LSA found that the **delay** of the notification of the initial breach to the LSA was not justified and found a violation of Article 33(1) GDPR [EDPBI:NL:OSS:D:2020:173]. Following this decision, data controllers shall notify each data breach after it occurs, even if the data controller considers it to be linked to other breaches.

## 4.2Communication of personal data breaches to the data subjects

Interesting on the issue of risk assessment is a document adopted by the Bulgarian SA, which developed a methodology for determining the level of risk in the event of a breach of personal data[40]. In one case where it serves as the LSA, the Bulgarian SA determined the severity of the risk to the rights and freedoms of data subjects according to this methodology, finding in the specific case that the rights and freedoms of the persons affected by the specific personal data breach were at "medium risk" [EDPBI:BG:OSS:D:2023:659].

In a case of hacking that resulted into a personal data breach of employees' data, the affected company informed the then existing and affected employees about the incident. The communication to them focused on the practical challenges that the incident posed to the individual employees and the actions that had been taken. However, the LSA did not conduct an analysis of whether this specific breach of personal data security is likely to present a high risk to the rights and freedoms of the employees. Given the way in which the company informed the data subjects affected by the breach, the LSA found the communication in line with Article 34(1) GDPR. It also agreed that as no customer personal data were affected, there was no need for notification to customers [EDPBI:DK:OSS:D:2021:288].

# 5. Concluding remarks

This report was dedicated to the analysis of decisions taken under Article 60 GDPR on Articles 32, 33 and 34 GDPR.

[40] Bulgarian SA, Methodology for determining the level of risk in the event of violations of the security personal data, as initially adopted by a decision of the CPDP on 29 May 2020, and amended and supplemented by a decision of the CPDP on 24 June 2021, available at https://www.cpdp.bg/userfiles/file/Kontrolna%20dejnost/Методика%20за%20оценка%20на%20риска%20при%20нарушение%20на%20сигурността.pdf (only in Bulgarian).

Most of the Final One-Stop-Shop Decisions studied in the context of this report relate to Article 32 GDPR, which also presents a lot of interest in the way in which LSAs assess the appropriateness of technical and organisational measures to ensure a level of security appropriate to the risk. In the near future, the CJEU is expected to shed some more light of the concept of the appropriateness of these measures.[41] Advocate General Pitruzzella argued that it would seem illogical to assume that the intention of the EU legislator was to impose on the controller the obligation to prevent any personal data breach irrespective of the diligence in the preparation of security measures[42] and that the mere existence of a personal data breach is not in itself sufficient to conclude that the technical and organisational measures implemented by the controller were not 'appropriate'.[43]

In their decisions on Article 32 GDPR, the LSAs carried out a case-by-case analysis of the technical and organisational measures implemented by the companies which were affected by a data breach. In most cases they also assessed the possible measures taken by the companies after the occurrence of the data breach and in several cases recommended appropriate measures. Despite the fact that the SAs analysed relevant measures on a case-by-case basis, we can draw some conclusions whether certain security measures are considered sufficient by the SAs or not. For instance, several SAs examined the establishment of proper access control mechanisms that can be ensured via the individual authentication of persons that are allowed to access specific (sets of) data. The lack of such clear access control mechanisms led various SAs to find violations of Article 32 GDPR [EDPBI:FR:OSS:D:2019:73; EDPBI:LT:OSS:D:2021:298; EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310; EDPBI:DK:OSS:D:2021:282; EDPBI:FR:OSS:D:2021:186].

The Final One-Stop-Shop Decisions cover a large variety of issues relating to security, such as ransomware, hacking, human errors, etc. The fact that SAs had to examine specific technical and organisational measures in concrete cases offers us the possibility to create a rich pool of security incidents and corresponding measures that have been found as appropriate or not appropriate in specific context. These can be a useful tool for SAs when assessing similar cases in the future.

The decisions relating to Articles 33 and 34 GDPR have been mostly dedicated to the examination by the LSAs of whether the notification of the personal data breach to the Supervisory Authority or the communication of the personal data breach to the data subjects have been in line with the obligations enshrined for data controllers in Articles 33 and 34 GDPR respectively.

Notification to the supervisory authority is not required when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In practice, as it also became clear from the analysis of the cases, data controllers tend to notify data breaches in most cases, instead of taking the risk of not notifying and then being found

[41] CJEU, Pending Case, Natsionalna agentsia za prihodite (C-340/21).

[42] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 35.

[43] AG opinion in C-340/21, Natsionalna agentsia za prihodite, 27 April 2023, para. 84.

later to be in violation.[44] One interesting finding is that data controllers shall notify each data breach after it occurs, even if the data controller considers it to be linked to other breaches [EDPBI:NL:OSS:D:2020:173].

Article 34 GDPR established an obligation for the data controllers to communicate the personal data breach to the data subjects without undue delay, only when the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects. Only in one case, the LSA carried out an evaluation of the specific risk imposed by the personal data breach to the rights and freedoms of the data subjects [EDPBI:BG:OSS:D:2023:659].

[44] Cédric Burton, 'Article 33. Notification of a personal data breach to the supervisory authority' in Kuner, Bygrave, and Docksey (eds.) The EU General Data Protection Regulation (GDPR): A Commentary (OUP 2020), p. 646.

European Data Protection Board