Skadden

Cybersecurity and Data Privacy Update

April 15, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

155 N. Wacker Drive
Chicago, IL 60606
312.407.0700

TaunusTurm
Taunustor 1
60310 Frankfurt am Main
Germany
49.69.74220.0

Data Protection Rulings by European Regulators Offer Insights Into Their Security Expectations

Executive Summary

- Valuable insights into the measures European regulators expect businesses to take to protect data privacy can be found in a report from the European Data Protection Board (EDPB) summarizing decisions under the EU's General Data Protection Regulation (GDPR).
- Although the decisions were made by authorities in different EU member states and the measures were discussed on a case-by-case basis tailored to specific data breaches, broader lessons can be drawn for other situations.
- The cases show once again the importance of having cybersecurity measures in place, regardless of whether the obligation is based on the GDPR or other applicable laws such as the Digital Operational Resilience Act or the NIS 2 Directive.[1]
- A proposal is pending to streamline the enforcement procedures for the GDPR.
- In a related matter, the European Court of Justice recently clarified that the occurrence of a personal data breach alone does not indicate that the technical and organizational measures taken by the controller were not appropriate.

Background of the GDPR's 'One-Stop-Shop' Mechanism

The EDPB case digest analyses the decisions adopted by EU member state supervisory authorities pursuant to Art. 60 GDPR. That provision created the so-called "one-stop-shop" mechanism, which allows businesses operating in multiple EU countries to interact primarily with the data protection authority in the country where they have their main establishment: the so-called Lead Supervisory Authority (LSA).

The one-stop-shop mechanism streamlines the process in the event of a data breach that has a cross-border impact, including those affecting data subjects in more than one EU member state. The LSA takes the lead in investigating and coordinating the response, while other concerned supervisory authorities are notified by the LSA and can provide input. Companies only need to coordinate with one authority, the LSA. Art. 60 GDPR requires the supervisory authorities to cooperate and adopt shared decisions in cases of cross-border data processing by a data controller.[2]

[1] Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[2] Pursuant to Art. 4 (23) GDPR, cross-border processing means either (a) processing of personal data which takes place in the context of the activities of establishments in more than one member state of a controller or processor in the Union where the controller or processor is established in more than one member state; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the EU but which substantially affects or is likely to substantially affect data subjects in more than one member state.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

Data Protection Rulings by European Regulators Offer Insights Into Their Security Expectations

The cases focus mainly on decisions concerning Art. 32 GDPR, which 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 organizational measures to ensure a level of security appropriate to the risk".

However, in their decisions under Art. 32 GDPR, the LSAs carried out case-by-case analyses of the technical and organizational 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, so the decisions also offer insights on the interpretation and application of Art. 33 and 34 GDPR, which cover data breach notifications.

The case digest was produced within the framework of the EDPB Support Pool Experts, which support supervisory authorities.[3] The digest is based on the register of final one-stop-shop decisions made publicly available online by the EDPB, accessed between 10 July and 31 August 2023.

Proposed Changes to GDPR Enforcement Regulations

In response to perceived shortcomings in the enforcement of the GDPR, in July 2023 the European Commission (EC) proposed changes to the procedures governing cross-border breaches involving data processing. The changes would harmonise procedural rights amongst involved parties, streamline and expedite collaboration amongst supervisory authorities, and elucidate the dispute resolution mechanism outlined in the GDPR.

The proposed rules aim to enhance privacy rights and increase legal clarity for businesses. The EC also emphasized quicker resolution of cases. However, it does not address substantive GDPR ambiguities or funding issues.

The EC's proposal suggests:

- Streamlining complaint handling.
- Introducing early scoping exercises for cooperation.
- Narrowly defining "relevant and reasoned objections" in order to limit disputes.
- Affording parties the right to be heard and access certain documents.
- Altering the rules governing urgent opinions and decisions under Art. 66(2) GDPR in ways that could restrict their scope.

On April 10, 2024, the European Parliament adopted its position on the EC's proposal with numerous changes to the EC's proposal, *e.g.*, broadening again the rules governing urgent opinions and decisions.

Key Themes in the Decisions

- **Lead supervisory authority (LSA):** In cases of data breaches involving cross-border processing, the data controller or processor does not have to coordinate with different data protection authorities, but can do so with the LSA, i.e., the supervisory authority in the country where the controller or processor has its main establishment.
- **Three categories of breach:** The majority of the decisions analysed involved one of three types of data breaches: (i) due to malicious attacks by external entities, (ii) due to insufficient practices and systems of organizations, and (iii) due to human error.
- **Preventive and remedial actions:** While Art. 32 GDPR does not explicitly distinguish between "preventive" and "remedial" measures, supervisory authorities commonly make that distinction in their decisions when evaluating measures implemented before and after a breach occurs.[4]

Appropriate and Inappropriate Measures

Because individual decisions involving breaches turn on specific company practices and systems, the measures discussed in the case digest are tailored to each specific breach. Nevertheless, the summaries offer guidance on what measures the LSAs may consider appropriate in other cases.

Breaches Due to Malicious Attacks by External Entities

Most of the cases involved external malicious attacks resulting in personal data breaches. The main findings are:

Preventive measures

- Data controllers are responsible for taking appropriate technical and organisational measures to ensure the security of personal data processing, including where they acquire a company that had already been compromised by a malicious attack before the acquisition.
- Organisational measures should include implementation of policies relating to data security (*e.g.*, policies against phishing and covering internet usage, personal devices, access control,

[3] More information on the EDPB Support Pool Experts is available here.

[4] This distinction may also arise from Art. 33(5) GDPR, which stipulates 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.

logging, etc.), as well as frequent awareness-raising campaigns and training for employees.

- Technical measures should include:
  - Encryption of personal data, especially sensitive data, during transmission and storage, using state-of-the-art algorithms and protocols, such as HTTPS, TLS, bcrypt, scrypt, Argon2, etc. The use of outdated or vulnerable encryption methods, such as HTTP, MD5, SHA1, etc., should be avoided.
  - Establishment of activity logs, particularly for access to the various servers of an information system, which enable the tracing of activities and the detection of any anomalies or events related to security, such as fraudulent access and misuse of personal data.
  - Implementation of effective access-control mechanisms, such as individual authentication of persons that are allowed to access specific (sets of) data, two/multi-factor authentication, password hashing, etc. The use of simple or weak passwords, or the transmission of passwords in clear text or via insecure channels, should be avoided.[5]
  - Effective countermeasures to prevent the compromising of an internet platform (such as a web shop) through the infiltration and execution of malware — measures such as command injection, the use of a Web Application Firewall (WAF or WSF) that analyses communication and blocks potentially harmful data traffic, penetration testing and auditing, etc.

Remedial measures

When addressing data breaches resulting from malicious attacks, LSAs also scrutinized the technical and organizational measures implemented by organizations post-breach. In complex cases, LSAs conducted comprehensive assessments of all measures undertaken by a company to determine their adequacy under Art. 32 GDPR.

Remedial measures should include, for example:

- Immediate isolation and blocking of the affected systems, servers, accounts or devices.
- Retrieval and security of the compromised data.
- Forensic analysis and reverse-engineering of the incident.
- Constant real-time monitoring of the activities, logs, systems and network traffic.
- Involvement of senior management, legal and IT teams.
- Hiring of external security experts or auditors.
- Notification and communication of the breach to the supervising authorities and the data subjects.
- Change of passwords and access codes.
- Installation of patches or updates.
- Switch to more secure cloud services.
- Email or push notification to inform users about unauthorized access attempts.
- Strengthening of access control and encryption.
- Establishment of new internal policies and procedures for security enhancement.

Breaches Due to Insufficient Practices and Systems

Several decisions involved personal data breaches due to insufficient company practices and systems. The main findings for this category of personal data breaches are:

Preventive measures

- Data controllers are responsible for taking appropriate technical and organisational measures to ensure the security of personal data processing, even if they outsource the security measures to data processors.
- Data controllers are required to monitor regularly the effectiveness of the technical and organisational measures implemented to ensure the security of the processing, including the measures taken by their processors.

Remedial measures

- To prevent accidental disclosure of personal data, it is recommended that multiple channels be used when sending personal data. For example, data subjects' information may be sent through a secure channel (*e.g.*, encrypted archives) while the passwords for accessing the data are sent via a separate channel (*e.g.*, SMS), to minimize the risk of exposure.
- Organisational measures should include the use of fictitious or anonymised data for IT testing, as well as the adoption of mandatory internal procedures for reporting and notifying personal data breaches. Those should specify individual steps to be taken after becoming aware of a breach, such as handling the incident, documenting the incident and taking corrective measures. The procedures should also include a method to carry out a risk assessment and notification of a breach.

[5] With regard to strong passwords, LSAs highlighted the guidelines of the German Federal Office for Information Security and the French data protection authority.

Data Protection Rulings by European Regulators Offer Insights Into Their Security Expectations

Breaches Due to Human Error

Given that technical systems frequently require the involvement of individuals, including company employees or end users, data breaches sometimes result from human errors.

Preventive measures

- Appropriate technical and organisational protections against data breaches, such as those due to the inadvertent disclosure of email addresses by email, should include technical solutions to avoid mass emails.
- Data controllers need to implement robust measures and conduct thorough testing to protect personal data from breaches caused by human error.
- Organisational measures should include the regular maintenance of existing systems.
- Regular testing of solutions to investigate and increase data security in systems to detect vulnerabilities and prevent subsequent breaches of Art. 32 GDPR.

Remedial measures

- Data controllers are responsible for implementing corrective measures to mitigate future incidents, including requiring employees to seek prior approval from a director and the data protection officer before sending external emails to more than three data subjects.
- Remedial measures should include further data protection training for the employee responsible for the error and, where appropriate, disciplinary action.
- Technical measures should be implemented to avoid possible compromise by human error. For example, before an email is sent via the "cc" function, the sender should be made aware and be able to reconsider.
- In case of the publication of non-critical personal data, prompt removal of faulty code or erasure of the data can be sufficient.

Related Decision of the European Court of Justice

Recently, the European Court of Justice also dealt with the question of the appropriateness of technical and organizational measures in accordance with Art. 32 GDPR.[6] The court ruled that unauthorized disclosure of personal data or unauthorized access to those data by a third party" is not sufficient, in itself, to imply that the technical and organisational measures implemented by the data controller in question were not "appropriate" within the meaning of Art. 24 and 32 GDPR.

This is a welcome development, as otherwise the controller could have been liable for the personal data breach regardless of the care taken in implementing security measures.

In practice, the LSAs' past decisions already follow this approach, in the sense that they assess on a case-by-case basis the technical and organisational security measures at stake.

[6] CJEU, 14 December 2023, (C-340/21).

Contacts

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Kata Éles
Associate / Frankfurt
49.69.74220.143
kata.eles@skadden.com

Research assistant **Elena Ntanas** assisted in preparation of this article.