Digital Legal Update

February 2025

Weinhold Legal

Below, we bring you the latest updates from the Digital and Cyber areas. If you have any questions regarding the information provided, please do not hesitate to reach out to us.

Contents

CJEU on Excessive or Unfounded Requests to Supervisory Authorities

The Court of Justice of the European Union (CJEU) issued a ruling on January 9, 2025, in case C-416/23, concerning the interpretation of Article 57(1)(f), Article 57(4), and Article 77(1) of the GDPR. The decision focused on the obligations of supervisory authorities in handling data subjects' complaints and the options available for responding to manifestly unfounded or excessive requests.

The CJEU confirmed that the term "request" in Article 57(4) GDPR also includes complaints submitted under Article 77(1) GDPR. This means that supervisory authorities may apply the options set out in Article 57(4) in cases of manifestly unfounded or excessive complaints by data subjects, namely imposing a reasonable fee or rejecting the complaint.

The Court emphasized that the mere number of complaints filed is not sufficient to consider requests as excessive. The supervisory authority must demonstrate that the complaints are submitted with an abusive intent, meaning they are not objectively justified by a genuine effort to protect the data subject's rights. For example, if a data subject files a large number of complaints against various controllers without a clear reason, this may indicate an abuse of rights.

The ruling confirmed that the supervisory authority has the discretion to choose between imposing a reasonable fee and rejecting the complaint. However, this decision must be justified and take all relevant circumstances into account. The authority should opt for a measure that is appropriate, necessary, and proportionate, with the imposition of a fee being considered a more lenient measure than outright rejection. Supervisory authorities must carefully assess whether complaints are filed in good faith or constitute an abuse of rights. The CJEU reaffirmed that data subjects have the right to effective protection of their rights, but this right must not be misused to overwhelm supervisory authorities.

CJEU on the Principle of Data Minimization

The Court of Justice of the European Union (CJEU) ruled on January 9, 2025, in case C-394/23, concerning the interpretation of Article 5(1)(c), Article 6(1)(b) and (f), and

Article 21 of the GDPR. The dispute involved the collection and processing of customer salutations ("Mr." or "Ms.") in online ticket sales by SNCF Connect. The association Mousse challenged this practice before the French supervisory authority (CNIL), which dismissed the complaint. Mousse then filed an annulment action against CNIL's decision before the Conseil d'État (French Council of State), which referred a preliminary question to the CJEU.

The Court confirmed that processing customer salutations ("Mr." or "Ms.") to personalize commercial communication based on gender identity is not objectively necessary to fulfill the contract for the provision of transport services. Less restrictive alternatives exist, such as using general and inclusive courtesy forms without reference to gender identity. Therefore, this processing cannot be justified under Article 6(1)(b) GDPR (necessity for contract performance).

Processing customer salutations cannot be considered necessary for the legitimate interests of the controller (e.g., marketing personalization) if:

- the controller did not inform customers about the legitimate interest pursued when collecting the data,
- the processing exceeds the necessary scope to achieve this interest,
- the fundamental rights and freedoms of customers (particularly the right to protection against discrimination based on gender identity) outweigh the interests of the controller.

The requirement of absolute necessity cannot be replaced by the data subject's right to object to the processing of personal data under Article 21 GDPR, as this is only a subsequent protective measure and cannot be used to justify processing that does not meet the conditions of lawfulness from the outset. The CJEU thus once again emphasizes the necessity of minimizing the collected data and thoroughly assessing whether the processing is genuinely necessary for the performance of a contract or for the legitimate interests of the controller.

EDPB Guidelines 01/2025 on Pseudonymization Open for Public Consultation

During its January 2025 plenary session, the European Data Protection Board (EDPB) published Guidelines 01/2025 on Pseudonymization for public consultation.

In these guidelines, the EDPB elaborates on the definition and practical use of pseudonymization as a tool that can help fulfill data protection obligations.

Pseudonymized data that can be attributed to a specific individual through additional information are still considered personal data. If the data controller or another entity can re-identify the data subject, the data remain personal data.

Pseudonymization can support compliance with the principle of data minimization, the implementation of data protection by design and by default (Article 25 GDPR), or the requirement for appropriate security measures corresponding to the risk (Article 32 GDPR). It may also facilitate the use of legitimate interests as a legal basis for processing (Article 6(1)(f) GDPR), provided all other GDPR conditions are met. Additionally, pseudonymization can help ensure the compatibility of further processing with the original purpose (Article 6(4) GDPR).

The guidelines analyze the technical and organizational measures and safeguards that must be implemented when using pseudonymization to ensure confidentiality and prevent unauthorized re-identification of individuals.

Digital Legal Update

February 2025

Weinhold Legal

The public consultation is open until February 28, 2025.

EDPB Report on the Coordinated Enforcement Framework (CEF) 2024 Joint Supervisory Action

The European Data Protection Board (EDPB) has published a report on the implementation of the right of access to personal data by data controllers. The report summarizes the findings of a series of coordinated national actions conducted in 2024 as part of the Coordinated Enforcement Framework (CEF) joint supervisory action. It identifies issues observed among some controllers and provides recommendations for improvement. A key aspect highlighted in the report is the awareness of controllers regarding EDPB Guidelines 01/2022 on the right of access and their actual compliance in practice. For each identified issue, the report includes a list of non-binding recommendations that controllers and data protection authorities should consider. The annex contains summaries of national supervisory actions, including inspections by the Czech DPA (ÚOOÚ), which assessed 22 controllers in the financial sector. The report emphasizes the need to improve awareness of Guidelines 01/2022, which guide controllers in understanding the right of access and its limitations.

Key Issues Identified in the Report:

- Lack of documented internal procedures for handling access requests by controllers.
- Inconsistent and excessive interpretation of limitations on the right of access, such as an overreliance on exemptions to automatically reject requests.
- Obstacles for data subjects, such as formal requirements or excessive demands for identification documents to exercise the right of access.

For each of these shortcomings, the report includes non-binding recommendations that controllers and data protection authorities (DPAs) should consider. The annex contains summaries of inspections conducted by national authorities, including the Czech DPA (ÚOOÚ), which assessed 22 controllers in the financial sector. The CEF 2025 action will focus on the implementation of the right to erasure ("right to be forgotten") under Article 17 GDPR.

EDPB Publishes Compendium on the OSS Mechanism and the Right of Access

The European Data Protection Board (EDPB) published a case compendium on the One-Stop-Shop (OSS) mechanism concerning the right of access to personal data on January 16, 2025. Since the GDPR came into effect, data protection authorities (DPAs) have closely collaborated on an increasing number of OSS decisions related to the right of access. This growing volume of decisions is reflected in the EDPB's public register (in accordance with Article 60 GDPR). The compendium provides practical examples of how the right of access is applied in different contexts, including cases involving fake profiles or accounts misusing data subjects' identities. It also references available EU-level guidelines, particularly EDPB Guidelines 01/2022 on the right of access, adopted on March 28, 2023. Additionally, relevant cases before the Court of Justice of the EU (CJEU) are discussed. The compendium summarizes how supervisory authorities interpret various aspects of the right of access in different situations and represents another step toward the harmonized and effective enforcement of the GDPR across the EU.

Digital Legal Update

February 2025

Weinhold Legal

EDPB Adopts Opinion on AI models

The European Data Protection Board (EDPB) issued Opinion 28/2024 on December 17, 2024, concerning the use of personal data for the development and implementation of artificial intelligence (AI) models. This opinion, titled "GDPR Principles Support the Responsible Development of AI," was prepared at the request of the Irish Data Protection Authority, aiming to achieve a harmonized approach across Europe. To gather the necessary input, the EDPB conducted stakeholder consultations and held discussions with the AI Office.

Given the broad scope of the Irish authority's request, the variety of AI models, and their rapid evolution, the opinion aims to provide guidance for analyzing specific situations.

The opinion focuses primarily on the following key areas:

- when and under what conditions AI models can be considered anonymous.,
- whether and how legitimate interest can serve as a legal basis for AI development or deployment,
- the consequences of developing an AI model using personal data that was processed unlawfully.

The opinion also addresses the use of data obtained from both first and third parties. Regarding the anonymity of AI models, the EDPB emphasizes that supervisory authorities should assess anonymity on a case-by-case basis. For an AI model to be considered anonymous, it must be highly unlikely that:

- it directly or indirectly identifies individuals whose data were used to create it, and
- personal data can be extracted from the AI model through queries (so-called prompts).

Regarding legitimate interest, the opinion provides general guidelines that supervisory authorities should consider when assessing whether legitimate interest is an appropriate legal basis for processing personal data in the development and implementation of AI models. For this assessment, the three-step test outlined in EDPB Guidelines 1/2024 on the processing of personal data based on legitimate interest, published in October 2024, applies. The test can be summarized as follows:

- identification of the legitimate interest pursued by the controller or a third party,,
- analysis of the necessity of processing for the pursued legitimate interest (also referred to as the "necessity test"), and
- assessment of whether the legitimate interest is overridden by the interests or fundamental rights and freedoms of data subjects.

The EDPB provides examples of processing based on legitimate interest, such as a conversational assistant designed to assist users or the use of AI to enhance cybersecurity. The opinion also states that if an AI model was developed using unlawfully processed personal data, this may affect the lawfulness of its deployment, unless the model has been properly anonymized.

Recommendations of the Czech Data Protection Authority (ÚOOÚ) on Camera Systems in Schools

The Office for Personal Data Protection (ÚOOÚ) has published Recommendation No. 1/2025 concerning camera systems in schools and educational institutions.

Digital Legal Update

February 2025

Weinhold Legal

This document is based on feedback and comments on the previously issued Methodology for the Design and Operation of Camera Systems in terms of data processing and personal data protection. The comments focused on specific or sectoral processing of personal data via camera systems, which were not suitable for inclusion directly in the original methodology.

The AI Office Publishes the Second Draft of the Code of Good Practice

The AI Office has published the second draft of the Code of Good Practice for general purpose AI models (GPAI), incorporating feedback on the first draft, which was released on November 14, 2024. The Code of Good Practice is part of the preparation for the implementation of the AI Act and is intended to serve as a guideline for providers of general purpose AI models on how to demonstrate compliance with the new regulations and effectively manage risks associated with GPAI. The third draft of the Code of Practice is expected to be published in the week of February 17, 2025, with the final version scheduled for May 2025.

Draft Act on Cybersecurity

The Draft Act on Cybersecurity is returning to the guarantee committee with proposed amendments, which will issue a resolution on them. The bill is then expected to proceed to the third reading in the Chamber of Deputies, where a vote will be held on the adoption of the proposed amendments.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Senior Advocate
Tereza.Hoskova@weinholdlegal.com

Daša Aradská
Advocate
Dasa.Aradska@weinholdlegal.com