Digital Legal Update

December 2024

Weinhold Legal

CJEU on violation of GDPR as an unfair commercial practice

The Court of Justice of the European Union (CJEU) in Lindenapotheke C-21/23 of 4 October 2024 provides important insights into the relationship between data protection and competition law.

The case concerned a dispute between two competing pharmacies, where one of them (Lindenapotheke) was selling medicines that were reserved for pharmacies on Amazon's online platforms, while the other pharmacy (DR), filed a lawsuit to stop the sale of these products, arguing that Lindenapotheke had breached the GDPR by failing to seek explicit consent from its customers with respect to processing their personal data, which included the processing of data that could indirectly result in sensitive data being disclosed regarding an individual, i.e. details concerning their personal health.

The CJEU confirmed that the personal data which are provided by customers when ordering medicines constitutes "health data" under Article 9 of the GDPR. Such conclusion was based on a broad interpretation of the term "health data", meaning that even data that may provide an indication of a person's health status with a certain likelihood falls within the protection provided under the GDPR.

The court also held that the GDPR does not prevent national legislation from allowing competitors to bring actions which are based on violations of the GDPR as **unfair commercial practices**. This means that competitors can assert their right to protection against unfair practices in the event of a breach of the data protection rules. The judgment thus confirms the importance of compliance with the GDPR **also within the context of compliance with competition rules.**

CJEU on the principle of data minimisation

On 4 October 2024, the Court of Justice of the European Union ruled in Case C-446/21 Meta Platforms Ireland, which dealt with data protection issues in the context of online marketing and advertising, specifically focusing on the practices of Meta Platforms Ireland.

The CJEU confirmed that companies must comply with the data **minimisation principle** under Article 5(1)(c) of the GDPR. This means that they can only process personal data that is necessary for a specific purpose. The judgment highlights the fact that Meta collected large amounts of personal data for targeted advertising, which is in fact contrary to this principle.

The court rejected Meta's argument that publicly available personal data may be processed for other purposes (personalized advertising) without the data subject's consent. It confirmed that the processing of such data must be limited to the purposes for which the data were originally collected, in accordance with the purpose limitation principle under Article 5(1)(b) GDPR. This judgment is thus considered a **significant development in the protection of personal data in the context of online marketing.**

CJEU on the publication of information in the commercial register

The judgment of the Court of Justice of the European Union (CJEU) in Case C-200/23, issued on 4 October 2024, deals with data protection issues in terms of the publication of information in the Commercial Register and its compliance with the GDPR.

Digital Legal Update

December 2024

Weinhold Legal

The case concerns a natural person who was a shareholder of a company in Bulgaria. In complying with the obligation to publish certain information about the company, the Articles of Association were sent to the Commercial Register, including the person's name and surname, identification number; ID card number; date and place of issuance of the ID card, as well as the address of the data subject and his signature. After the data had been published, the data subject applied to the Bulgarian Commercial Register (Agencia po vpisvanijata) with a request to have them erased.

The CJEU in this case concluded that, while there is a legal obligation to publish certain information in the Commercial Register under Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 on certain aspects of company law, the protection of personal data under the GDPR must also be considered. The Court emphasised that the right to the protection of personal data cannot be automatically subordinated to the transparency requirements of the Commercial Register.

According to the CJEU, the data subject has the **right to request the erasure of his or her personal data**, unless there are compelling legitimate grounds which override his or her interests and rights and freedoms under Article 21(1) of the GDPR, and which must be demonstrated by the controller. It further emphasised the **principle of proportionality**, which requires that a balance be made between the right to the protection of personal data and the public's right of access to the information.

EDPB Guidelines 02/2024 on public consultation

On 3 December 2024, for the purpose of public consultation the European Data Protection Board (EDPB) published Guidelines 02/2024, clarifying the rules for the transfer of personal data to third-country authorities when there are situations concerning the transfer or disclosure of data which is not authorised by EU law under Article 48 of the GDPR. In these guidelines, the EDPB explains Article 48 of the GDPR and clarifies how organisations can best assess under what conditions they can respond to requests for the transfer of personal data made outside the EU in accordance with the GDPR; the public consultation will run until 27 January 2025.

EDPB approves EU Data Protection Seal

The EDPB has approved the certification of the EU Data Protection Seal pursuant to Article 45(5) of the GDPR. This **certification** helps organisations in demonstrating their compliance with the GDPR, and further assists data subjects with regard to trusting products, services, processes or even systems for which organisations process their personal data.

First review of the EU-US Data Privacy Framework

Following the Commission's report of 9 October 2024, the European Data Protection Board issued a report on the first review of the European Commission's adequacy decision in relation to the EU-US Data Privacy Framework (DPF), i.e. the **legal framework for the transfer of personal data to the US** under Article 45 of the GDPR. This adequacy decision on the EU-US DPF previously entered into force on 10 July 2023, and a commitment was made by the Commission to conduct the first review within the first year of its entry into force. The aim of the review was to verify whether the adequacy decision is still factually and legally justified, as well as to highlight areas for improvement so as to ensure that an adequate level of protection is achieved with regard to personal data transfers between the EU and the US.

Digital Legal Update

December 2024

Weinhold Legal

EDPB

- noted the low number of complaints lodged by data subjects under the so-called redress mechanism, suggesting the need for increased monitoring and controls of the US authorities' compliance with the adequate level of protection;
- called on the US authorities to develop clear guidance for companies who are certified under the DPF on compliance requirements, esp. regarding HR data;
- stressed the importance of the principles of necessity and proportionality in terms of access to personal data; and
- recommended that future reviews of decisions on the appropriate level of protection should take place every three years or sooner.

AI Authority has published a draft code of practice

The Artificial Intelligence Authority (AI Authority) has published the first draft of a code of practice for general purpose AI models (GPAI). The final version of the Code is expected to be published in May 2025. The rules for general AI models under Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulation (EC) No. 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (the AI Act), the AI Act will enter into force pursuant to Article 113(b) of the AI Act in August 2025. The Code of Practice aims to:

- to facilitate compliance with the rules for generic models set out in the AI Act; and
- to play a key role in guiding the future development and deployment of trusted and safe generic AI models

Key aspects of the Code include:

- guidance on how providers of generic AI models can respect copyright throughout the lifecycle of their models;
- taxonomy of systemic risks;
- risk assessment methodologies; and
- mitigation measures for providers of advanced generic AI models that may pose systemic risks.

Although compliance with the Code is not mandatory, it is expected to play a **key role in demonstrating compliance with the AI Act**.

AI Authority launches public consultation on AI system definition and prohibited practices

The AI Authority has launched a public consultation process on future guidance on the definition of an AI system and prohibited AI practices that the AI Act believes pose unacceptable risks. The public consultation will run until 11 December 2024.

These guidelines will assist the competent national authorities, as well as providers and introducers, in terms of compliance with AI Act rules on such prohibited practices, which will take effect on 2 February 2025. The final version of these guidelines is expected to be published by the AI Office in early 2025.

Digital Legal Update

December 2024

Weinhold Legal

Draft law on cyber security

The draft law on cyber security, which has been addressed in the past few weeks by various parliamentary committees, has been returned to the Chamber of Deputies for a second reading together with their respective amendments.

The National Office for Cyber and Information Security has prepared a calculator to serve as a tool for better orientation as to whether a given company, or the services it provides, will be affected by the upcoming law on cyber security. The calculator is also intended to help navigate the issue of whether the provision of regulated services will be subject to a regime of lower or higher obligations. The result generated by this online tool is only indicative, while the final assessment of the relationship of the new Cybersecurity Act in respect of a given entity is at the entity's own discretion.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Senior Advocate
Tereza.Hoskova@weinholdlegal.com

Daša Aradská
Advocate
Dasa.Aradska@weinholdlegal.com