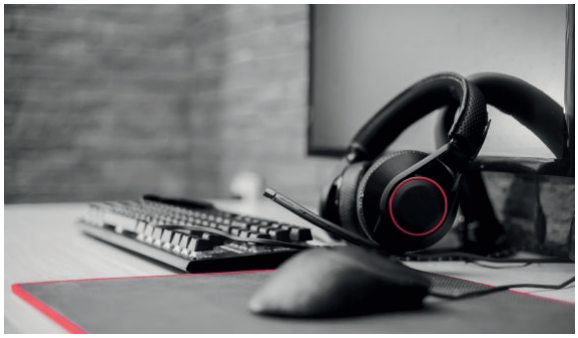
ADVANT Beiten

Privacy Ticker

January 2025



+++ DORA IN FORCE +++ ECJ: GENDER INFORMATION UNNECESSARY WHEN PURCHASING TICKETS +++ ECJ: COLLECTIVE AGREEMENTS DO NOT CREATE A LEGAL BASIS +++ IRELAND: FINE OF EUR 251 MILLION AGAINST META DUE TO DATA BREACH +++ EDSA ADOPTS GUIDELINES ON PSEUDONYMISATION +++

1. Changes in Legislation

+++ DORA IN FORCE +++

The Regulation on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act, DORA) has been directly applicable in all EU Member States since 17 January 2025. From this date, affected companies must comply with all relevant obligations (see Privacy Ticker July 2024). Almost all supervised institutions and companies in the European financial sector are subject to DORA and must now implement the requirements related to cybersecurity, ICT risks and digital operational resilience. For instance, by 11 April 2025 at the latest, financial companies must submit the ICT information register to BaFin. The BaFin, as the supervisory authority in Germany, can impose effective and deterred sanctions in the event of violations of DORA.

To the BaFin website regarding DORA (dated 24 January 2025, in German)

To the wording of DORA (dated 14 December 2022)

2. Case Law

+++ ECJ: GENDER INFORMATION UNNECESSARY WHEN PURCHASING TICKETS +++

The European Court of Justice (ECJ) has ruled that specifying the title "Mr." or "Ms." is not necessary when purchasing tickets online. It is generally possible to provide the transportation service without specifying the gender identity in relation to the title. Personalisation of business communication, such as the use of courtesy formulas, also does not require the indication of gender identity. The ECJ has left open the question of whether data processing can be justified on the basis of a company's legitimate interests. However, the Court indicated that commercial direct marketing, as a legitimate interest, does not require the indication of salutation or gender identity. Furthermore, the ECJ ruled that the data subject's right to object should not be taken into account when balancing legitimate interests.

To the ECJ ruling (dated 9 January 2025, C-394/23)

+++ ECJ: COLLECTIVE AGREEMENTS DO NOT CREATE A LEGAL BASIS +++

The European Court of Justice (ECJ) has clarified the data protection requirements for collective agreements. According to the ruling, collective agreements, such as works agreements, must comply not only with the requirements of Article 88 GDPR but also with Articles 5, 6, and 9 GDPR. This includes the data protection principles and the requirements for the lawfulness of processing, as well as those for sensitive data. These prerequisites ensure that collective agreements do not undermine the level of protection established by the GDPR. Accordingly, works agreements do not serve as an independent legal basis, but rather specify the legal bases outlined in the GDPR. Furthermore, the ECJ has granted courts broad power to review the necessity of data processing as regulated in collective agreements.

To the ECJ ruling (dated 19 December 2024, C-65/23)

3. Regulatory Investigations and Enforcement Actions

+++ IRELAND: FINE OF EUR 251 MILLION AGAINST META DUE TO DATA BREACH +++

The Irish Data Protection Commission (DPC) has fined Meta Platforms Ireland Limited a total of EUR 251 million. Meta had implemented the "View as" feature on the social network Facebook, which allowed users to view their own account from the perspective of another user. Cybercriminals exploited a vulnerability in this function to gain access to around 29 million Facebook accounts, including around 3 million in the EU. Personal data such as name, email address and gender were tapped. The fine was imposed for violating the principles of privacy by design and privacy by default. In addition, the notification of the data breach was incomplete, and the incident was not sufficiently documented.

To the DPC press release (dated 17 December 2024)

+++ ITALY: FINE OF EUR 15 MILLION AGAINST OPENAI FOR LACK OF LEGAL BASIS AND INTRANSPARENCY +++

The Italian data protection authority Garante per la Protezione dei Dati Personali (GPDP) has imposed a fine of EUR 15 million on OpenAI, the US operator of ChatGPT. The GPDP found that the AI-based chatbot ChatGPT processed personal data without a sufficient legal basis. OpenAI also failed to provide adequate information to users and did not implement age verification mechanisms to ensure the proper protection of children. In addition to the fine, the GPDP ordered OpenAI to carry out a six-month communication campaign across radio, television, newspapers and the internet to promote transparency in the processing of personal data.

To the GPDP press release (dated 20 December 2024)

To the administrative fine notice of the GPDP (dated 2 November 2024, in Italian)

+++ NETHERLANDS: FINE OF EUR 4.75 MILLION AGAINST NETFLIX FOR LACK OF INFORMATION +++

The Dutch data protection authority Autoriteit Persoonsgegevens (AP) has fined the streaming service Netflix EUR 4.75 million. An investigation by the AP revealed that Netflix had not sufficiently informed its users about the processing of their personal data between 2018 and 2020. In particular, Netflix did not clearly communicate the legal basis and purposes of data processing, which data was shared with third parties, how long data was stored, and what measures Netflix took for transfers to third countries. Requests for the right of access by the data subjects were also not answered with sufficient clarity. Netflix has appealed against the fine.

To the AP press release (dated 18 December 2024)

To the AP's fine notice (dated 26 November 2024)

4. Opinions

+++ EDPB ADOPTS GUIDELINES ON PSEUDONYMISATION +++

In its new guidelines, the European Data Protection Board (EDPB) outlines the meaning, scope and benefits of pseudonymisation. The EDPB clarifies that pseudonymised data is still considered personal data. Therefore, the GDPR is applicable if the data can be linked to a person through additional information. However, the EDPB also highlights that pseudonymisation, as a technical and organizational measure, can reduce risks and support the use of legitimate interests as a legal basis for processing. In addition, the guidelines provide various use cases and analyse technical measures and safeguards associated with the use of pseudonymisation.

To the press release of the EDPB (dated 17 January 2025)

To the EDSA guidelines (dated 16 January 2025)

+++ EDPB: OPINION ON THE PROCESSING OF PERSONAL DATA IN AI MODELS +++

The European Data Protection Board (EDPB) has published an opinion on the data protection aspects of processing personal data in AI models. The EDPB asserts that AI models often contain personal data, even if they were not specifically designed, trained or developed to process personal data. For such models, the EDPB recommends that the competent supervisory authorities conduct a case-by-case assessment and provides some guidance on when AI models could be considered as anonymous. The EDPB also discusses the processing of data based on legitimate interests and outlines potential measures to safeguard the rights of data subjects. Lastly, the EDPB addresses the consequences of unlawful data processing.

To the press release of the EDPB (dated 18 December 2024)

To the EDPB opinion (dated 17 December 2024)

+++ LOWER SAXONY DATA PROTECTION AUTHORITY: CRITICISM OF THE CONSENT MANAGEMENT REGULATION +++

The State Commissioner for Data Protection of Lower Saxony has expressed clear criticism of the Consent Management Regulation adopted on 20 December 2024, which is expected to come into force on 1 April 2025 (see blog post from September 2024). The regulation aims to reduce and simplify consent banners (also known as cookie banners) on websites, which are often seen as disruptive. However, the authority criticizes the fact that consent banners will still be necessary, and that the regulation only covers consent under the Telecommunications Digital Services Data Protection Act, but not under the GDPR. Additionally, the use of consent management services by website operators will remain voluntary. As a result, the authority assumes that the new regulation will bring little change of the current consent practices on websites.

To the press release of the authority (dated 27 December 2024, in German)

Your Contacts

If you have any questions, please address the ADVANT Beiten lawyer of your choice or contact the ADVANT Beiten Privacy Team directly:

Office Frankfurt
Mainzer Landstrasse 36 | 60325 Frankfurt am Main

Dr Andreas Lober

+49 69 756095-582
vCard

Susanne Klein, LL.M.

+49 69 756095-582
vCard

Lennart Kriebel

+49 69 756095-582
vCard

Fabian Eckstein, LL.M.

+49 69 756095-582
vCard

Jason Komninos, LL.M

+49 69 756095-582
vCard

Mirjam Kaiser

+49 69 756095-582
vCard

Office Dusseldorf
Cecilienallee 7 | 40474 Dusseldorf

Mathias Zimmer-Goertz

+49 211 518989-144
vCard

Christian Frederik Döpke, LL.M.
+49 211 518989-144
vCard

Office Munich
Ganghoferstrasse 33 | 80339 Munich

Katharina Mayerbacher

+89 35065-1363
vCard

Dr Birgit Münchbach

+89 35065-1312
vCard

EDITOR IN CHARGE
Dr Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

BB-Datenschutz-Ticker@advant-beiten.com
www.advant-beiten.com

Update Preferences | Forward

Please note

This publication cannot replace consultation with a trained legal professional. If you no longer wish to receive information, you can unsubscribe at any time.

Imprint

This publication is issued by Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811
For more information see:
www.advant-beiten.com/en/imprint

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH is a member of ADVANT, an association of independent law firms. Each Member Firm is a separate and legally distinct entity, and is liable only for its own acts or omissions.