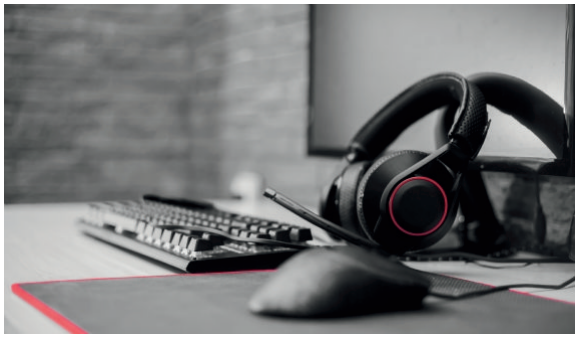
ADVANT Beiten

Privacy Ticker

October 2024



**+++ DRAFT OF AN EMPLOYEE DATA PROTECTION ACT +++
ECJ: ORDER INFORMATION CAN REPRESENT HEALTH DATA +++
ECJ: SENSITIVE DATA MAY NOT BE USED FOR PERSONALISED ADVERTISING +++ EUR 310 MILLION FINE AGAINST LINKEDIN FOR UNLAWFUL PROCESSING FOR ADVERTISING PURPOSES +++**

1. Changes in Legislation

+++ DRAFT OF AN EMPLOYEE DATA PROTECTION ACT +++

The Ministry of Labour and the Ministry of the Interior have drafted a new Employee Data Protection Act. The draft of this so-called "Beschäftigtendatengesetz" is available to us but has not yet been officially published by the ministries. The law has a broad scope of application and applies to all data processing in the employment relationship. There is an exemplary catalogue of criteria for weighing up interests as well as standard examples of effective consent. Furthermore, it is clarified that collective agreements (e.g. works agreements) cannot constitute an independent legal basis. In addition, a fundamental prohibition on the utilisation of unlawfully obtained information is to be introduced. For typical case constellations, such as job interviews or the use of surveillance software, the draft contains regulations on which data the employer may process, when video surveillance is permitted or how data may be shared within the group. Extended labelling and information obligations are to become mandatory when using AI.

To the article on handelsblatt.com (dated 17 October 2024, in German)

+++ CYBER RESILIENCE ACT ADOPTED +++

The European Council has adopted the Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). The regulation introduces EU-wide cybersecurity requirements for the design, development, manufacture and placing on the market of hardware and software products (see Privacy Ticker March 2024). The aim is to avoid overlapping requirements due to different legislation in the EU Member States. Products that are directly or indirectly connected to another device or a network should therefore be more secure throughout their entire life cycle. The Cyber Resilience Act has yet to be published in the Official Journal of the EU and will enter into force 20 days later. The regulations will apply 36 months after coming into force, although some provisions will apply earlier.

To the press release of the European Council (dated 10 October 2024)

Text of the Cyber Resilience Act (dated 23 October 2024)

2. Case Law

+++ ECJ: ORDER INFORMATION CAN REPRESENT HEALTH DATA +++

The European Court of Justice (ECJ) has defined the term "health data" in concrete terms, taking a very broad understanding as a basis. The background to this was the sale of non-prescription medicines on Amazon by a pharmacist. A competitor saw this as an unfair practice, as health data, such as name and delivery address, had been processed without the corresponding consent. According to the ECJ, order information for medicines is already health data, as the health status of a natural person can be deduced by combining the therapeutic indication of the medicine with the delivery address and name. This applies regardless of who the order is placed for, as the health status of third parties can also be disclosed under certain circumstances. In addition, the ECJ confirms that competitors are also entitled to take action against competitors for data protection violations.

To the judgment of the ECJ (dated 4 October 2024, C-21/23)

+++ ECJ: NO OBLIGATION OF THE SUPERVISORY AUTHORITIES TO TAKE REMEDIAL ACTION +++

The European Court of Justice (ECJ) has ruled that supervisory authorities

are not always obliged to take remedial action in the event of breaches ofthe GDPR, as they are granted a level of discretion. In principle, supervisory authorities must process complaints from data subjects withthe due diligence required to comply with the GDPR and select suitable remedies, taking into account all the circumstances of the individual case. However, they are not obliged to take action or impose a fine in every case of a breach of the GDPR. The authorities' obligation only extends as far as it is possible to respond to the breach in an appropriate manner. If the breach has already been remedied, for example if the controller has already taken the necessary measures on their own initiative, authorities can refrain from taking measures at their discretion.

To the judgment of the ECJ (dated 26 September 2024, C-768/21)

To the press release of the ECJ (dated 26 September 2024)

+++ ECJ: APOLOGY CAN BE SUFFICIENT COMPENSATION FOR DAMAGE +++

According to the European Court of Justice (ECJ), an apology can serve as an appropriate form of compensation if it fully compensates for the non-material damage suffered. In the underlying case, the plaintiff claimed damages from the Latvian consumer protection authority because it had published a video imitating him without his consent. Although the national courts found an infringement, they refused to award financial compensation and only ordered an apology. The ECJ confirmed this view and ruled that an apology can also constitute independent or supplementary compensation for non-material damage in order to comply with the principle of effectiveness.

To the judgment of the ECJ (dated 4 October 2024, C-507/23)

+++ ECJ: SENSITIVE DATA MAY NOT BE USED FOR PERSONALISED ADVERTISING +++

The European Court of Justice (ECJ) has ruled that social networks such as Facebook may not process all personal data for the purposes of targeted advertising. The case was brought by data protection activist Maximilian Schrems, who objected to the processing of data relating to his sexual orientation by Facebook. Schrems himself had made information about his sexual orientation public in a panel discussion. The ECJ found that Facebook was authorised to process this data in compliance with the provisions of the GDPR. However, Facebook was not entitled to process other data about sexual orientation, in particular in order to evaluate it and offer personalised advertising. Furthermore, the

principle of data minimisation means that a social network may not analyse and process data indefinitely and without differentiating between its types for the purposes of targeted advertising.

To the judgment of the ECJ (dated 4 October 2024, C-446/21)

3. Regulatory Investigations and Enforcement Actions

+++ FINE OF EUR 310 MILLION AGAINST LINKEDIN FOR UNLAWFUL PROCESSING FOR ADVERTISING PURPOSES +++

The Irish Data Protection Commission (DPC) has imposed a fine of EUR 310 million on LinkedIn. The background to the decision was the unlawful processing of personal data for the purpose of analysing behaviour and displaying personalised advertising. The processing carried out by LinkedIn could neither be based on voluntary and informed consent nor on legitimate interests or contract fulfilment. Furthermore, the DPC considered the principle of fairness to have been violated and the information obligations with regard to the basis for processing to have been insufficiently fulfilled. In addition to imposing a fine, it issued a warning to the social business network and instructed LinkedIn to bring its processing in line with the GDPR.

To the DPC press release (dated 24 October 2024)

+++ FINE OF EUR 91 MILLION AGAINST META FOR STORING PASSWORDS +++

The Irish Data Protection Commission (DPC) has fined Meta Platforms Ireland Limited EUR 91 million and issued a warning. As part of a routine security investigation, Meta discovered that a large number of social media users' passwords were inadvertently stored in plain text in Meta's internal systems and reported the data protection incident to the Irish authority in March 2019. The DPC based its decision on the breach of the integrity and confidentiality of the data processing and the security of the processing due to inadequate technical and organisational measures. In addition, Meta had neither reported the incident immediately nor documented it as required by the GDPR.

To the DPC press release (dated 27 September 2024)

To the Meta press release (dated 21 March 2019)

4. Opinions

+++ EDPB: RESPONSIBILITIES OF THE CONTROLLER IN THE ASSIGNMENT OF DATA PROCESSORS +++

The European Data Protection Board (EDPB) has issued an opinion on the obligations of the controller when commissioning processors and sub-processors. Among other things, it comments on the extent of the controller's obligation to identify all processors and sub-processors. It also specifies the scope of the review and documentation of suitable guarantees for the selection and use of processors. Another point is the possibility for the controller to review the contract of the first processor with further sub-processors. Finally, third country transfers in the processing chain and the exceptions to the obligation to follow instructions are also considered.

To the press release of the EDPB (dated 9 October 2024)

To the opinion of the EDPB (dated 7 October 2024)

+++ EDPB: GUIDELINES ON THE BALANCING OF INTERESTS +++

The European Data Protection Board (EDPB) has published new guidelines analysing the criteria set out in Art. 6 (1) lit. f GDPR that controllers must meet in order to lawfully process personal data on the basis of legitimate interest. To this end, the controller must pursue a legitimate interest, the processing must be necessary and the interests of the controller or a third party must be weighed against the interests of the data subjects. The guidelines explain how this assessment should be carried out in practice, with reference also being made to specific contexts such as fraud prevention, direct marketing and information security. The document also highlights the relationship between this legal basis and a number of data subject rights under the GDPR.

To the press release of the EDPB (dated 9 October 2024)

To the guidelines of the EDPB (dated 8 October 2024)

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.