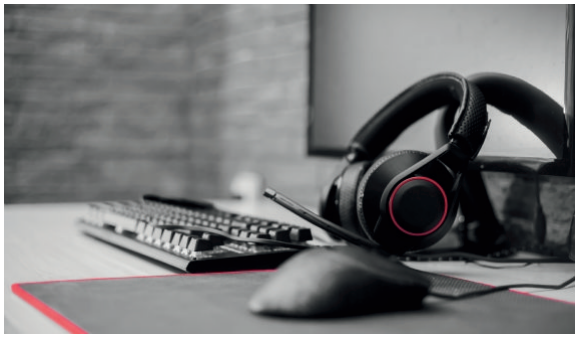
ADVANT Beiten

Privacy Ticker

September 2024



+++ FEDERAL GOVERNMENT ADOPTS COOKIE REGULATION +++ HIGHER REGIONAL COURT OF MUNICH: DATA BREACH JUSTIFIES TERMINATION OF EMPLOYMENT WITHOUT NOTICE +++ FINE OF EUR 30.5 MILLION AGAINST CLEARVIEW +++ FINE OF EUR 3.2 MILLION DUE TO META-PIXEL ON WEBSITE +++ DATA PROTECTION CONFERENCE: TRANSFER OF PERSONAL DATA IN ASSET DEALS +++

1. Changes in Legislation

+++ FEDERAL GOVERNMENT ADOPTS COOKIE REGULATION +++

On 4 September 2024, the German government adopted the so-called Consent Management Regulation, which aims to reduce the number of cookie banners and improve the user experience on the Internet. The ordinance is based on Section 26 of the German Telecommunications Data Protection Act (TDDDG). It governs the procedure for recognizing and the general requirements for so-called consent management services. Recognized consent management services shall make it possible, for example, for users to specify their cookie preferences once when accessing a website and for this setting to be saved permanently. However, a blanket default setting for all websites or digital services is not possible under the regulation. The integration of recognized consent management services by providers of digital services is voluntary.

To the text of the regulation (dated 4 September 2024, in German)

To our blog post (dated 9 September 2024)

2. Case Law

+++ HIGHER REGIONAL COURT OF MUNICH: DATA BREACH JUSTIFIES TERMINATION OF EMPLOYMENT WITHOUT NOTICE +++

The Higher Regional Court of Munich has ruled that the repeated forwarding of internal company information such as pay slips, documents relating to commission claims, invoices or bank enquiries relating to anti-money laundering by a member of the Executive Board to his own private email address constitutes a severe breach of duty which justifies extraordinary termination of the employment without notice. Forwarding the emails and storing them on the private email account constituted processing under data protection law that was not covered by consent or any other legal basis. Not every violation of the GDPR is an important reason within the meaning of Section 626 of the German Civil Code (BGB), which justifies termination without notice. In this case, however, the transferred documents contained sensitive data of third parties, including other employees. The court also took into account the frequency with which the documents were forwarded. This had led to the trust relationship with the company being shattered in an irreparable way due to the forwarding of the highly sensitive data in breach of data protection laws.

To the judgment of the Higher Regional Court of Munich (dated 31 July 2024, 7 U 351/23 e, in German)

+++ REGIONAL COURT OF TRAUNSTEIN: NO CLAIM AGAINST SOCIAL NETWORK FOR DATA PROCESSING SOLELY IN EUROPE +++

The Regional Court of Traunstein has ruled that a social media user cannot demand that the network operator processes and stores data exclusively within the EU. The user demanded compensation, injunctive relief and deletion of his data because he considered the transfer of data to the USA to be unjustified. The court did not agree with this view. The search for users who are outside the EU can only work if cross-border data exchange is possible. This also applies if the user himself has no contacts outside the EU. A user must accept that it is part of the business decision of the operator of a social network to also process data in the USA, especially as no one is forced to use the platform in question. For

global social networks, it is therefore generally necessary to transfer data to third countries to fulfil the contract, provided that the conditions for data transfer to third countries in accordance with the GDPR are met.

To the judgment of the Regional Court of Traunstein (dated 8 July 2024, 9 O 173/24, in German)

+++ ADMINISTRATIVE COURT OF SCHLESWIG: DASHCAM VIDEOS ON YOUTUBE MUST BE PIXELATED +++

According to a decision by the Administrative Court of Schleswig, dashcam videos published on YouTube must be pixelated if personal data (people or vehicle license plates) are visible. The plaintiff is a YouTuber and filmed road traffic using a camera mounted on the roof of his car. He later published the videos on his YouTube channel. The plaintiff defended himself against an order from the competent data protection authority, which ordered him to pixelate the recordings and provide information to data subjects. The court ruled in favor of the authority with regard to the obligation to pixelate personal data. In this respect, the protection of personal rights and the right to informational self-determination of the data subjects prevailed. However, the court did not declare the authorities' requirement to comply with the information obligations directly in the video recordings to be lawful. Rather, it was sufficient to provide the information on a website or YouTube channel.

To the judgement of the Administrative Court of Schleswig (dated 7 August 2024, 8 A 159/20, in German)

3. Regulatory Investigations and Enforcement Actions

+++ FINE OF EUR 30.5 MILLION AGAINST CLEARVIEW +++

The Dutch data protection authority (Autoriteit Persoonsgegevens) has imposed a fine of EUR 30.5 million on the American company Clearview AI. Clearview offers facial recognition services for intelligence agencies and investigative authorities. Clearview's customers can provide camera images in order to determine the identity of the persons depicted in the

images. Clearview has a database of more than 30 billion photos of people, including from the Netherlands. In the opinion of the data protection authority, Clearview obtained the data unlawfully. The data analyzed from the photos is also biometric data and therefore particularly sensitive data. Furthermore, Clearview did not properly fulfill its duty to provide information and did not respond to requests for information. In addition, Clearview had not appointed a representative for the EU and had been uncooperative towards the authority.

To the press release (dated 3 September 2024) and the fine notice of the Dutch Data Protection Authority

+++ FINE OF EUR 3.2 MILLION DUE TO META-PIXEL ON WEBSITE +++

The Swedish data protection authority Integritetsskydds myndigheten (IMY) has imposed a fine of the equivalent of EUR 3.2 million on the company Apoteket AB, which operates an online store for drugstore products and non-prescription medicines in Sweden. The company had used the meta pixel analysis tool on its website to evaluate and improve its marketing on Facebook and Instagram. A function of the Meta Pixel had been activated unintentionally, which resulted in more data being processed and transmitted to Meta than originally intended. Among other things, data on the purchase of over-the-counter medication, self-tests and treatments for sexually transmitted diseases and sex toys were transmitted. Data relating to health or sex life is subject to special protection under Art. 9 GDPR. The authority's investigation found that Apoteket AB had not taken appropriate technical and organizational measures to ensure an adequate level of protection for customers' personal data.

To the press release of the Swedish Data Protection Authority (dated 30 August 2024, in Swedish)

To the fine notice (dated 29 August 2024, in Swedish)

4. Opinions

+++ DATA PROTECTION CONFERENCE: TRANSFER OF PERSONAL DATA IN ASSET DEALS +++

In a new resolution, the German Conference of Independent Federal and State Data Protection Supervisory Authorities has set out the conditions under which the transfer of data in a company acquisition by way of an asset deal is possible in compliance with data protection laws. In doing so, it has categorized the data transfers based on the individual stages of a company acquisition, from contract initiation to contract conclusion. In addition to differentiating between the transfer of customer data, employee data and supplier data, the paper highlights various legal bases that can justify data transfers. Apart from the legitimate interest, the authorities consider consent to be necessary in individual cases, but also the fulfillment of the contract as a possible legal basis for the transfers. Finally, the resolution contains general information on company acquisitions in the context of data protection, such as the allocation of the roles of the purchaser and seller under data protection law or information obligations. The new resolution replaces the previous resolution on the same topic from 2019.

To the authorities' resolution (dated 11 September 2024, in German)

+++ DATA PROTECTION CONFERENCE: RESOLUTION ON THE USE OF FACIAL RECOGNITION SYSTEMS BY SECURITY AUTHORITIES+ ++

In a recent resolution, the Conference of Independent Federal and State Data Protection Supervisory Authorities criticizes the use of automated biometric facial recognition systems by security authorities in public spaces. In the opinion of the authorities, the existing provisions of the Code of Criminal Procedure do not provide a sufficient legal basis for the use of these systems. This not only constitutes a data protection violation, but also an intensive encroachment on the fundamental rights of data subjects, the intensity of which depends on the type of data analyzed, the technology used and the degree of automation. In addition, facial recognition could lead to serious consequences for the persons concerned, such as deprivation of liberty, in the event of false recognition.

Insofar as the evaluation is therefore not already based on the requirements of the AI Act (see Privacy Ticker May 2024), the authorities are calling for the creation of specific legal bases for the use of facial recognition systems. The European Data Protection Board (EDPB) has also set out strict requirements in its guidelines on the use of facial recognition technology in law enforcement.

To the authorities' resolution (dated 20 September 2024, in German)

To the guidelines of the EDPB (dated 26 April 2023)

+++ DATA PROTECTION CONFERENCE: GUIDELINES ON DATA PROCESSING IN CONNECTION WITH RADIO-BASED METERS +++

In a new guideline, the German Conference of Independent Federal and State Data Protection Authorities clarifies questions regarding the legality of the radio-controlled collection and transmission of consumption data, e.g. from remotely readable cold water, electricity, heating or hot water meters. According to the authorities, meter and consumption-related data is always personal if it can be assigned to a specific person, e.g. by means of a device identification number or via the tenancy agreement. This also applies in the case of a multi-person household, as consumption can still allow conclusions to be drawn about the lifestyle of individual persons. In addition to the apartment or building owners, the data controller under data protection law could also be the responsible energy or water supplier or the metering point operator. The legal basis for data processing can be found, for example, in the Metering Point Operation Act and the Heating Costs Ordinance. In addition, a template for fulfilling the information obligations is provided.

To the authorities' guidelines (dated 16 August 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.