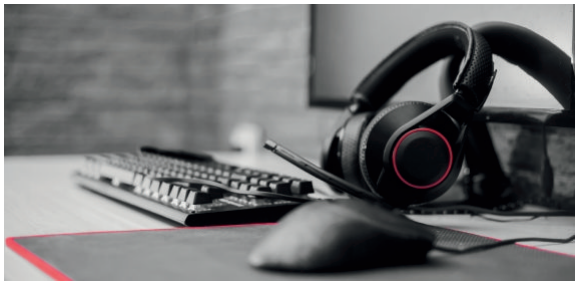
ADVANT Beiten

Privacy Ticker

May 2022



+++ Agreement on the Digital Services Act +++ Consumer Protection Associations Can Sue for GDPR Breaches +++ EDBP Publishes Guidelines on Calculation of Fines +++

1. Changes in Legislation

+++ EU INSTITUTIONS AGREE ON DIGITAL SERVICES ACT +++

In the so-called trilogue procedure, representatives of the EU Parliament, the Member States and the Commission have agreed on a final version of the "Digital Services Act". The regulation is to contain new regulations in the areas of e-commerce, consumer and data protection law (see AB Privacy Ticker January 2022). In particular, the regulation will prohibit advertisers from collecting and analysing sensitive data such as political or sexual orientation for targeting purposes. Profiling of minors is also to be generally prohibited. In addition, so-called "dark patterns", i.e. the possibility of manipulating users' decisions, are to be restricted. In case of violations, there is a threat of fines similar to those imposed by the GDPR, namely up to 6 per cent of the platform provider's total turnover in the previous business year.

To the report on Heise.de (dated 10 May 2022, in German)

2. Case Law

+++ ECJ: CONSUMER PROTECTION ASSOCIATIONS WITH AUTHORITY TO FILE LAWSUITS IN DATA PROTECTION VIOLATIONS +++

The European Court of Justice (ECJ) had to decide on the question of whether consumer protection associations may permissibly file lawsuits

themselves under the GDPR. This was based on a legal dispute of the German Federation of Consumer Organisations (*Verbraucherzentrale Bundesverband*) against Meta (formerly Facebook) before the Federal Supreme Court. The plaintiff demanded an injunction because Meta had violated data and consumer protection regulations as well as competition rules by making free third-party games available to users. The Federal Supreme Court saw a need for clarification on the question of whether not only public data protection authorities should be entitled to a general right to take action against data protection violations. The ECJ granted the plaintiff a so-called right of action by associations to ensure a high level of protection of personal data.

To the ECJ ruling (dated 28 April 2022, C-319/20)

+++ FEDERAL SUPREME COURT SUBMITS QUESTION TO ECJ ON ABUSIVE GDPR INFORMATION CLAIMS +++

The Federal Supreme Court has submitted several questions on the right to information (Art. 15 GDPR) to the ECJ. The reason for this is a lawsuit filed by a patient against a dentist. The plaintiff is seeking the free surrender of a copy of all his medical records held by the defendant. The defendant believes that it only has to provide a copy of the patient's records against reimbursement of costs. The Federal Supreme Court wants the ECJ to clarify, among other things, whether the controller is obliged to provide the data subject with an initial copy of his or her data free of charge if the data subject does not request the copy in order to pursue data protection purposes. In fact, the plaintiff requested the information primarily for the preparation of medical malpractice proceedings. This could be considered an "excessive" request (Art. 12(5) GDPR). In a similar case, the Nuremberg Higher Regional Court had already rejected a claim for information as abusive (see AB Privacy Ticker April 2022).

To the request for a preliminary ruling (dated 29 March 2022, VI ZR 1352/20, in German)

+++ NEURUPPIN LABOUR COURT: EUR 1,000 DAMAGES IF EMPLOYEE DATA IS NOT DELETED FROM THE WEBSITE AFTER LEAVING THE COMPANY +++

The Neuruppin Labour Court awarded the plaintiff non-material damages for late deletion of data. The employee had left the company and had requested the employer to remove all personal data from the company's website. As her former employer did not immediately comply with this request, she demanded EUR 5,000 as compensation, whereupon theemployer paid EUR 150. The Court considered only a total of EUR 1,000 in damages to be appropriate, taking into account the case law of the lower courts, even though the plaintiff had not alleged any immaterial damage. In the Court's view, this was not necessary, as Art. 82 GDPR also includes a warning and deterrent function. In addition to the breach of data protection law, the Court also held that the obligation to delete the data arose directly from the employment contract as a secondary obligation (section 241 (2) German Civil Code).

To the judgement of the Neuruppin Labour Court (dated 14 December 2021, 2 Ca 554/21, in German)

3. Regulatory Investigations and Enforcement Actions

+++ BAVARIAN DATA PROTECTION AUTHORITY DOES NOT IMPOSE A FINE DESPITE SIGNIFICANT VIOLATION +++

The Bavarian Data Protection Authority did not impose a fine on a car rental company despite a supposed serious violation, which allowed external access to about three million customer data (a total of about 10 TBytes of data) due to a configuration error in a backup server. This probably included addresses and telephone numbers of celebrities and politicians. According to the authority, the imposition of sanctions or other measures is not necessary if the operator of an open server can prove that there was only a "limited, possibly even individually identifiable and thus specifically assessable number of actors" who had access to the data, for instance "by evaluating log files together with transmitted data volumes". In the case at hand, analyses of the car rental company's network traffic had only determined "a low probability of occurrence of a retrieval with the purpose of misuse of data". Thus, neither a fine nor an individual notification of the data subjects was necessary.

To the report on heise.de (dated 6 May 2022, in German)

+++ FRENCH DATA PROTECTION AUTHORITY IMPOSES MILLION DOLLAR FINE FOR DISCLOSURE OF HEALTH DATA +++

The French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) has imposed a fine of EUR 1.5 million on a provider of software and related services for medical laboratories. The company had stored personal data without encryption on a server to which access was possible without sufficient authentication. This exposed health data, including full names, national insurancenumbers and genetic data, of nearly 500,000 individuals. CNIL considered this to be a significant breach of the obligation to take adequate organisational and technical measures to protect data (Art. 32 GDPR). In addition, the company had collected more data than necessary and had concluded an inadequate data processing contract with its clients.

To the administrative fine notice of the authority (dated 15 April 2022, in French)

To the EDPB press release (dated 15 April 2022)

4. Opinions

+++ EDPB: NEW GUIDELINES FOR THE CALCULATION OF GDPR FINES +++

The European Data Protection Board (EDPB) has adopted new guidelines on the calculation of GDPR fines. A five-step method is intended to promote harmonisation and transparency in the calculation of fines by data protection authorities in the individual Member States. In the guidelines, the EDPB assesses, among other things, various aggravating or mitigating circumstances and explains applicable fine frameworks with examples. For data protection controllers, the guidelines can provide valuable conclusions for risk assessment and conduct following a (potential) data protection breach. The guidelines are initially open for public consultation until 27 June 2022.

To the EDSB guidelines (dated 12 May 2022)

+++ DSK DEMANDS THE INTRODUCTION OF AN EMPLOYEE DATA PROTECTION ACT +++

The Conference of the Independent Data Protection Authorities of the German Federal and State Governments (DSK) has called for the creation of an Employee Data Protection Act. The DSK sees the need for such a law in particular due to the risks associated with digitalisation. In particular, the DSK considers the following areas to be in need of regulation: the use of algorithmic systems including artificial intelligence, the limits of behavioural and performance monitoring, the framework conditions for consent, regulations on data processing based on collective agreements, regulations on the relationship between the various legal bases for data collection and prohibitions on the use of evidence. In the area of employee data protection, the GDPR grants member states to create more specific regulations for the processing of personal data,which was previously implemented by section 26 German Federal Data Protection Act.

To the DSK resolution (dated 29 April 2022, in German)

+++ DSK DEMANDS GUEST ACCESS IN E-COMMERCE +++

The DSK has determined that the principle of data economy must be particularly observed in eCommerce (Art. 5 (1) lit. c) GDPR). Therefore, it demands that it must be possible for customers in eCommerce to purchase goods or services with a mere "temporary guest access". If the customer has no interest in a permanent relationship and an associated customer account, he or she must be given the option of merely setting up a guest account. In the case of guest access, only such data should be processed as is necessary for the concrete conclusion of the contract. Via this guest access, customers should be enabled to perform an equivalent ordering process as those who opt for a permanent customer account.

To the resolution of the DSK (dated 24 March 2022, in German)

+++ DATA PROTECTION AUTHORITIES WANT TO PROHIBIT ADDRESS TRADING +++

According to media reports, some federal and state data protection authorities want to take joint action against address trading, which is used to target customers by post. They are of the opinion that passing on addresses for marketing purposes without the consent of the data subjects is no longer permitted under the GDPR. In particular, the State Commissioner for Data Protection and Freedom of Information of Baden-Wuerttemberg states that in practice, data subjects are regularly not sufficiently informed about the data processing involved in address trading.

To the report on tagesschau.de (dated 3 May 2022, in German)

EDITOR IN CHARGE
Dr Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH
BB-Datenschutz-Ticker@advant-beiten.com
www.advant-beiten.com

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 96 756095-582
E-Mail

Susanne Klein, LL.M.

+49 69 756095-582
E-Mail

Lennart Kriebel

+49 69 756095-582
E-Mail

Fabian Eckstein, LL.M.

+49 69 756095-582
E-Mail

Office Munich
Ganghoferstrasse 33 | 80339 Munich

Katharina Mayerbacher

+89 35065-1363
E-Mail

Office Dusseldorf
Cecilienallee 7 | 40474 Dusseldorf

Mathias Zimmer-Goertz

+49 211 518989-144
E-Mail

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

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.