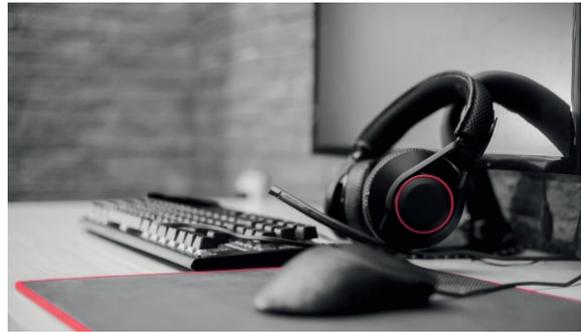


Privacy Ticker

April 2024



**+++ HEALTH DATA USE ACT IN FORCE +++ ECJ: COMPANIES
LIABLE FOR DAMAGES IN CASE OF DATA PROTECTION BREACHES
BY EMPLOYEES +++ DELAYED GDPR INFORMATION CONSTITUTES
A BREACH OF COMPETITION THAT CAN BE WARNED +++ FINE OF
EUR 2.9 MILLION AGAINST GREEK POST AFTER CYBER ATTACK
+++ EDPB STATEMENT ON CONSENT OR PAY MODELS ON ONLINE
PLATFORMS +++**

1. Changes in Legislation

+++ HEALTH DATA USE ACT IN FORCE +++

The 'Act on the Use of Health Data for Research Purposes in the Public Interest and for the Data-based Further Development of the Healthcare System' (Health Data Use Act) was passed by the German Parliament in December 2023 and came into force on 26 March 2024. The new law regulates the use of health data nationwide and creates a new legal basis for this purpose. For instance, treatment data may be used for quality assurance and research purposes as well as for statistical and health reporting purposes. The law also allows cancer registry data to be linked with data from the Health Research Data Centre. For transnational health research projects, the possibility of a lead data protection supervisory authority is being introduced. In addition, the law implements research confidentiality subject to criminal prosecution. The Hessian Commissioner for Data Protection and Freedom of Information had dealt with the law in detail in advance, assessed it positively and, according to its own statement, will advocate a data protection by design and by default and standardised interpretation of the new law.

[To the press release of the Hessian authority \(dated 28 March 2024, in German\)](#)

[To the text of the Health Data Use Act \(dated 26 March 2024, in German\)](#)

2. Case Law

+++ ECJ: COMPANIES LIABLE FOR DAMAGES IN CASE OF DATA PROTECTION VIOLATIONS BY EMPLOYEES +++

The European Court of Justice (ECJ) has confirmed and differentiated its case law on liability for non-material damages in the event of data protection breaches. In the underlying case, the plaintiff defended himself against the use of his data for advertising purposes by juris GmbH, a legal platform. Although he had lodged an objection to advertising, the company repeatedly sent him personalised advertising. The plaintiff demanded compensation and argued that he had lost control of his data. The defendant's argument was that employees had acted contrary to instructions. The ECJ initially confirmed that a data protection breach does not automatically lead to a claim for damages but that the plaintiff must prove specific damage. Such damage could also be the loss of control over data, whereas there is no de minimis limit. Furthermore, the ECJ states that a company cannot exculpate itself on the grounds that an employee has acted contrary to instructions and this has resulted in a data protection breach. The mere misconduct of employees is not sufficient to exempt them from liability as the controller. Finally, the ECJ clarifies that the criteria for assessing fines do not also apply to the assessment of damages and that multiple offences in the same processing operation do not lead to an increase in damages.

[To the ECJ ruling \(dated 11 April 2024, C-741/21\)](#)

+++ ECJ: TC STRING OF THE IAB EUROPE IS PERSONAL DATA +++

The European Court of Justice (ECJ) has ruled that a TC string encoding a user's consent preferences regarding the processing of its personal data qualifies as personal data insofar as it allows the data subject to be identified. The IAB Europe is a non-profit association and has developed a system for online advertising auctions. These are carried out using a real-time bidding system that enables the automated auctioning of advertising space based on user profiles. The user's consent is obtained via consent management before targeted advertising is displayed. Consent is encoded and stored in a string consisting of a combination of letters and characters, known as a 'Transparency and Consent String' (TC string), which is shared with personal data brokers and advertising platforms. The ECJ has now confirmed that the TC string contains information about an identifiable user and is considered personal data within the meaning of

the GDPR. This holds true in particular if the TC string can be linked to an identifier such as the IP address of the user device. In this context, it is irrelevant whether IAB Europe can directly access the personal data. Furthermore, the ECJ categorised IAB Europe as a joint controller. It is sufficient for the association to determine the purposes and means of data processing together with its members. It is not necessary for the association to have its own access to the data.

[To the press release of the ECJ \(dated 7 March 2024\)](#)

[To the ECJ ruling \(dated 7 March 2024, C 604/22\)](#)

+++ FCJ: GMBH MANAGING DIRECTOR HAS NO RIGHT TO HAVE HIS DATE OF BIRTH AND PLACE OF RESIDENCE DELETED FROM THE COMMERCIAL REGISTER +++

According to the Federal Court of Justice (FCJ), the GDPR does not grant the managing director of a GmbH the right to have his date of birth and place of residence removed from the commercial register. The plaintiff was entered in the commercial register as the managing director of a GmbH with his date of birth and the place of residence stated at the time of registration. He applied to have the data removed and justified this with a personal threat, e.g. through kidnapping, as his professional activity involved handling explosives. The FCJ rejects the claim. A claim for erasure could arise from Art. 17 GDPR. However, the claim is ruled out as the entry of the data in the commercial register is provided for and required by law. The publication of the data in the commercial register serves the security, fairness, and ease of legal transactions. In the opinion of the court, the interests of the data subject must take second place. Furthermore, a right to removal of the data does not arise from the right to restriction of processing pursuant to Art. 18 GDPR or the right to object pursuant to Art. 21 GDPR.

[To the ruling of the Federal Court of Justice \(dated 23 January 2024, II ZB 7/23, in German\)](#)

+++ DELAYED GDPR INFORMATION CONSTITUTES A BREACH OF COMPETITION THAT CAN BE WARNED +++

The Düsseldorf Regional Court has ruled that a delay in providing information in accordance with Art. 15 GDPR constitutes a breach of competition law that can be cautioned by a consumer organisation. The defendant operates the Peek & Cloppenburg online store and had requested a private individual to pay outstanding debts. The alleged

customer rejected this on the grounds that he had been the victim of identity theft and in return demanded information from the defendant in accordance with Art. 15 GDPR. The defendant only responded to this after two months and thus not within the one-month period stipulated by law. The consumer organisation called in by the data subject demanded that the defendant refrain from providing late information to consumers in the future. The court affirms the claim, as late information constitutes a breach of data protection and also a breach of competition law. According to the court, the obligation to provide information and the relevant deadline serve to protect consumers and constitute market conduct regulations within the meaning of the Unfair Competition Act (UWG). Consumer organisations are therefore entitled to prosecute such violations by companies.

[To the judgement of Dusseldorf Regional Court \(dated 15 March 2024, 34 O 41/23, in German\)](#)

3. Regulatory Investigations and Enforcement Actions

+++ FINE OF EUR 2.9 MILLION AGAINST GREEK POST AFTER CYBER ATTACK +++

The Greek data protection authority has imposed a fine of EUR 2.9 million on the Hellenic Post Office, the Greek postal service. It had fallen victim to a ransomware attack that affected the data of 4 to 5 million people. This included private customers, employees, and credit companies. Some of the tapped data was also published on the darknet. During its investigation, the authorities discovered that the attack had been carried out via a security vulnerability in the IT system. Due to financial problems, the Greek Post had not adequately secured its security systems. In the opinion of the data protection authority, Greek Post had also not taken sufficient technical measures to defend against cyber attacks. To make matters worse, there had already been other attacks in the past, but Greek Post had not taken the opportunity to significantly improve security. And it had also failed to regularly test the functionality of its IT systems.

[To the DPA's press release \(dated 28 February 2024, in Greek\)](#)

[To the administrative fine notice of the DPA \(dated 28 February 2024, in Greek\)](#)

4. Opinions

+++ EDPB STATEMENT ON CONSENT OR PAY MODELS ON ONLINE PLATFORMS +++

The European Data Protection Board (EDPB) has published a statement on the effectiveness of consent to the processing of personal data for behavioral advertising in the context of so-called "consent or pay" models on online platforms. Users of a website are usually given two options to be able to read the website's content: Either they take out a paid subscription or they consent to their data being used for profile-based and individualized advertising. The data protection conference assessed these models as permissible in principle in March 2023 ([see Privacy Ticker April 2023](#)). The EDPB takes a much more critical view of the model and demands that users be given a real choice. In the opinion of the EDPB, most of the models currently introduced do not meet the requirements for effective consent. The EDPB believes that paid use without advertising tracking is not an equivalent alternative. Rather, providers should offer consumers another free alternative without behavioral advertising. The EDPB has announced that it will develop guidelines on "consent or pay" models.

[To the EDPB press release \(dated 17 April 2024\)](#)

[To the statement of the EDPB \(dated 17 April 2024\)](#)

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. This data protection ticker was created in cooperation with the ADVANT partner law firms Nctm and Altana.

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 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](#)



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](#)



[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.

© Beiten Burkhardt

Rechtsanwaltsgesellschaft mbH

All rights reserved 2024

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.