

# Privacy Ticker

November 2025



**+++ OMNIBUS PACKAGE: EU PLANS TO AMEND GDPR, DATA ACT, AI ACT, ETC. +++ CROATIA: EUR 4.5 MILLION FINE FOR INTRA-GROUP DATA TRANSFER TO THIRD COUNTRY +++ HESSIAN DATA PROTECTION AUTHORITY: MICROSOFT 365 CAN BE USED IN COMPLIANCE WITH DATA PROTECTION LAW +++**

## 1. Changes in Legislation

**+++ OMNIBUS PACKAGE: EU PLANS TO AMEND GDPR, DATA ACT, AI ACT, ETC. +++**

The EU Commission has published drafts for so-called "Digital Omnibus Regulations". The plan is to amend the GDPR, Data Act, AI Act, e-Privacy Directive, and other EU legislation. The initiative aims to reduce bureaucratic hurdles and standardize digital legislation. With regard to the GDPR, the draft includes a revision of the definition of personal data. Data should not be considered personal for an entity if that entity itself has no means to identify the data subject, even if third parties would be able to do so (so-called relative personal reference). In addition, the reporting requirements for data breaches are to be adjusted. Notifications to the supervisory authorities will only be required if there is a high risk to the rights of the data subjects. In addition, the reporting deadline is to be extended from 72 to 96 hours and the procedure is to be standardized using unitary forms. The cookie rules from the ePrivacy Directive will be transferred to the GDPR with regard to personal data, more exceptions will be added, and the modalities for requesting consent will be specified. In addition, the draft envisages the possible admissibility of data processing for the training of AI models based on legitimate interest.

[To the draft regulation on GDPR, Data Act, ePrivacy, etc. \(dated 19 November 2025\)](#)

[To the draft regulation on the AI Act \(dated 19 November 2025\)](#)

## **+++ GERMAN PARLIAMENT PASSES NIS 2 IMPLEMENTATION ACT+++**

On November 13, 2025, the German parliament passed the law implementing the NIS 2 Directive. The aim of the law is to adapt the level of cybersecurity in Germany to the increased threat posed by disinformation, sabotage, and espionage. The scope of the regulations has been expanded: Around 30,000 companies in Germany are to be classified as "essential" or "important" entities and will have to meet strict security requirements in the future. Key obligations include the implementation of state-of-the-art risk management measures and a multi-stage reporting procedure for security incidents (24-hour early warning, 72-hour reporting to the authority). In addition, management will now be legally obliged to monitor the implementation of the measures and undergo regular training.

[To the press release of the Federal Government \(dated 21 November, 2025, in German\)](#)

[To the press release of the Federal Office for Information Security \(dated 13 November 2025, in German\)](#)

## **2. Case Law**

### **+++ FEDERAL COURT OF JUSTICE: PERMISSIBLE TRANSFER OF POSITIVE DATA TO SCHUFA +++**

The Federal Court of Justice has ruled that mobile phone providers may lawfully transfer so-called positive data, including master data and information about the conclusion or termination of a contract, to credit agencies such as SCHUFA if there is a legitimate interest pursuant to Art. 6 (1) lit. f GDPR. A consumer association had filed a lawsuit against a mobile phone company to prevent it from passing on data to SCHUFA. The defendant argued that there was a legitimate interest in the transfer in order to prevent fraud attempts. Especially in the case of "postpaid" mobile phone contracts, high-value smartphones are regularly sent out at the beginning of the contract, which entails a high risk of fraud. The Federal Court of Justice holds that the injunction was too broad. The transfer of positive data was neither an unreasonable interference with the fundamental rights of consumers nor could it be replaced equally effectively by less severe means. The information was not sensitive and did not allow any conclusions to be drawn about the private lives of the affected individuals.

[To the ruling of the Federal Court of Justice \(dated 14 October 2025, VI ZR 431/24, in German\)](#)

### **+++ ADMINISTRATIVE COURT OF BERLIN: DUTY TO PROVIDE INFORMATION ON DATA ORIGIN IN LETTERSHOP PROCEEDINGS+++**

The Administrative Court of Berlin has ruled that there does not have to be a joint controllership between the advertising company and the address dealer in the so-called "lettershop procedure". In the lettershop procedure, the advertiser does not have direct access to the data records; instead, the advertising material is created and sent by a service provider (address dealer). The plaintiff had been issued with a data protection warning in official proceedings because the authority assumed that there had been unlawful data processing. The court overturned the warning because it considered the plaintiff to be the wrong addressee for the measure. Although the plaintiff appeared to be responsible for the advertising campaign to the outside world, as its name and corporate design were used, it did not determine the means of processing, which is an essential prerequisite for joint controllership.

[To the ruling of the Administrative Court of Berlin \(dated 14 October 2025, 1 K 74/24, in German\)](#)

## **3. Regulatory Investigations and Enforcement Actions**

### **+++ FEDERAL DATA PROTECTION AUTHORITY: RECOGNITION OF THE FIRST CONSENT MANAGEMENT SERVICE +++**

The Federal Commissioner for Data Protection and Freedom of Information has recognized the first consent management service in accordance with the German Consent Management Regulation. The Regulation, which was introduced on the basis of Section 26 of the German Act on Data Protection and Privacy in Telecommunications and Digital Services, is intended to improve the user experience on the internet. The idea behind the legislation was to replace traditional cookie banners with centrally managed services. Users would enter their cookie preferences once, and participating websites would be able to access them automatically. The Regulation was intended to reduce the flood of cookie banners, which, according to surveys, annoy a large proportion of internet users ([see blog post from 9 September 2024](#)).

[To the press release of the Federal Commissioner for Data Protection and Freedom of Information \(dated 4 November 2025, in German\)](#)

### **+++ CROATIA: EUR 4.5 MILLION FINE FOR INTRA-GROUP DATA TRANSFER TO THIRD COUNTRY +++**

The Croatian data protection authority Agencija za zaštitu osobnih podataka (AZOP) has imposed a fine totalling EUR 4.5 million on a telecommunications company. The company had transferred personal data of its users to a processor in Serbia, which was part of the group of companies and performed software management tasks. The transfer was initially covered by standard contractual clauses from 2020 to 2022. However, after that, there were no corresponding agreements, meaning that the Serbian processor had unrestricted access to sensitive data from more than 800,000 individuals without any legal basis. Prior to the data transfer, the controller had not carried out an adequate risk assessment, nor had the data subjects been informed of the transfer. In addition, the authority criticized the excessive processing of employee data, in particular the storage of copies of employees' identity cards.

[To the AZOP press release \(dated 14 November 2025, in Croatian\)](#)

### **+++ FINLAND: FINES IMPOSED ON BANKS FOR SECURITY DEFICIENCIES IN ONLINE BANKING +++**

The Finnish data protection authority Tietosuojavaltuutetun toimisto has imposed fines on two credit institutions for significant security gaps in online banking. S-Bank must pay EUR 1.8 million and Aktia Bank EUR 865,000. In both cases, technical changes led to massive malfunctions in authentication: At S-Bank, customers were able to log into online banking with someone else's access data for months, while at Aktia Bank, after a system adjustment in January 2023, it was temporarily possible to log into external services where sensitive personal data of other people was displayed. In total, a large proportion of S-Bank's customer base and around 350 Aktia Bank customers were directly impacted. In both cases, the authority found violations of Articles 5, 25, and 32 of the GDPR, as the banks had inadequately planned, implemented, and tested new functions and technical changes and had not taken indications of misconduct into account in a timely manner. In the case of S-Bank, a previous reprimand and a parallel sanction by the financial supervisory authority were also taken into account in determining the amount of the fine.

[To the EDPB report on S-Bank \(dated 18 November 2025\)](#)

[To the Finnish authority's fine notice regarding S-Bank \(dated 8 September 2025, in Finnish\)](#)

[To the EDPB report on Aktia Bank \(dated 18 November 2025\)](#)

[To the Finnish authority's fine notice regarding Aktia Bank \(dated 23 October 2025, in Finnish\)](#)

## 4. Opinions

### **+++ HESSIAN DATA PROTECTION AUTHORITY: MICROSOFT 365 CAN BE USED IN COMPLIANCE WITH DATA PROTECTION LAW +++**

The Hessian Commissioner for Data Protection and Freedom of Information has published a report on the use of Microsoft 365 (M365), which shows that M365 can be used in compliance with data protection regulations under certain conditions. Microsoft offers M365 as a cloud service in which Microsoft is the processor and the customer is the controller. The basis for this is a Data Protection Addendum (DPA). In 2022, the German Data Protection Conference criticized the fact that the DPA did not regulate seven points in accordance with the GDPR. According to the Hessian authority, Microsoft has since made significant adjustments: Almost all data is now processed in the European Economic Area, data transfers to the US are secured by the EU-US Data Privacy Framework or standard contractual clauses, and the DPA has been revised, particularly for public authorities. In addition, Microsoft provides additional information materials such as the "M365 Kit", which supports controllers in their documentation. The seven original points of criticism raised by the Data Protection Conference, such as unclear information on data types and purposes, insufficient rights, security measures, deletion requirements, and subcontractor information, as well as inadmissible transfers to third countries, have been addressed by Microsoft's measures.

[To the press release of the Hessian Commissioner for Data Protection and Freedom of Information \(dated 14 November 2025, in German\)](#)

[To the report of the Hessian Commissioner for Data Protection and Freedom of Information \(dated 15 November 2025, in German\)](#)

# 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

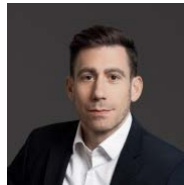
[vCard](#)



### 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

+49 89 35065-1363

[vCard](#)



### Dr Birgit Münchbach

+49 89 35065-1312

[vCard](#)



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 privacy ticker was created in cooperation with the ADVANT partner law firms Nctm and Altana.

### EDITOR IN CHARGE

Susanne Klein, LL.M. | Rechtsanwältin

©Beiten Burkhardt

Rechtsanwaltsgesellschaft mbH

[BB-Datenschutz-Ticker@advant-beiten.com](mailto:BB-Datenschutz-Ticker@advant-beiten.com)

[www.advant-beiten.com](http://www.advant-beiten.com)



## E-Mail weiterleiten

**Please note:** If you no longer wish to receive information, you can [unsubscribe](#) at any time.

### Imprint

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH

Ganghoferstrasse 33, 80339 Munich, Germany

Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No: DE11218811

Tel.: +49 89 35065-0, Fax: +49 89 35065-123 | E-Mail: [munich@advant-beiten.com](mailto:munich@advant-beiten.com)

Here you will find our complete imprint: [www.advant-beiten.com/en/imprint](http://www.advant-beiten.com/en/imprint) and our privacy

policy: [www.advant-beiten.com/en/privacy-protection](http://www.advant-beiten.com/en/privacy-protection)