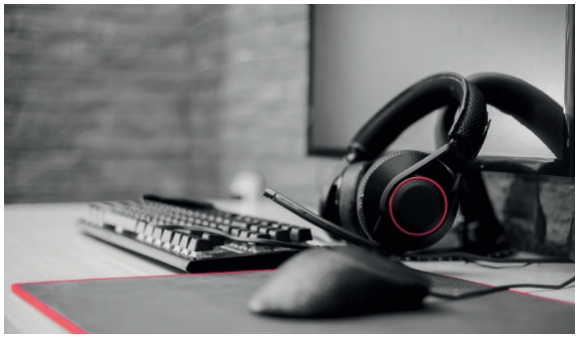
ADVANT Beiten

Privacy Ticker

August 2025



+++ FEDERAL COURT OF JUSTICE DENIES DAMAGES FOR HYPOTHETICAL RISKS +++ POLAND: EUR 3.96 MILLION FINE AGAINST MCDONALD'S FOR DATA LEAK +++ BFDI ON THE USE OF SOCIAL NETWORKS BY THE FEDERAL ADMINISTRATION+++ EU COMMISSION USES MICROSOFT 365 IN COMPLIANCE WITH DATA PROTECTION LAW +++

1. Case Law

+++ FEDERAL COURT OF JUSTICE DENIES DAMAGES FOR HYPOTHETICAL RISKS +++

The German Federal Court of Justice has further defined its case law on damages in accordance with Art. 82 GDPR. In the underlying case, the defendant city had transmitted an acknowledgement of receipt containing the plaintiff's personal data to the administrative court by unencrypted fax despite the plaintiff's objection. The plaintiff considered this to be a breach of data protection and demanded payment of monetary compensation. The court rejected the plaintiff's claim for non-material damages because he had not shown that he had suffered any non-material damage. A purely hypothetical risk of misuse by an unauthorized third party could not lead to compensation. Contrary to the plaintiff's view, a loss of control does not already exist because it was theoretically possible to intercept the personal data due to the unencrypted transmission by fax. Rather, there was only a purely hypothetical risk that did not justify any non-material damage.

To the judgment of the Federal Court of Justice (dated 13 May 2025, VI ZR 186/22, in German)

+++ HIGHER REGIONAL COURT SCHLESWIG-HOLSTEIN ON META'S AI TRAINING +++

The Higher Regional Court of Schleswig-Holstein has rejected an application by the Dutch consumer protection foundation Stichting Onderzoek Marktinformatie (SOMI) for an interim injunction against the use of certain customer data by Facebook and Instagram for AI training due to a lack of urgency. In an application dated 27 June 2025, SOMI argued that the actual use of the data had begun without the users' consent and that the interests and fundamental rights of consumers outweighed Meta's interest in processing the data for AI training purposes. Meta had already started using this data in May 2025 and invoked a legitimate interest in the development of its AI technologies. The court ruled that the matter was not as urgent as to justify an injunction, since the use of the data had already begun a month earlier and Meta's intention to use the data had been known since April 2025. The court referred SOMI to possible proceedings on the merits.

To the judgment of the Higher Regional Court of Schleswig-Holstein (dated 12 August 2025, 6 UKl 3/25, in German)

To the press release of the court (dated 12 August 2025, in German)

2. Regulatory Investigations and Enforcement Actions

+++ POLAND: EUR 3.96 MILLION FINE AGAINST MCDONALD'S DUE TO DATA LEAK +++

The Polish data protection authority Urząd Ochrony Danych Osobowych (UODO) has imposed a fine of around EUR 3.96 million on McDonald's Polska. The proceedings were initiated following a data leak reported in July 2020. Personal data of employees had been publicly accessible in an unsecured database, allowing unauthorized persons to access work schedules and ID card information, among other things. The authority found that neither McDonald's as the controller nor its processor had regularly reviewed the security measures. Measures such as pseudonymization were only implemented after the incident became known. The UODO considered this to be a breach of the principle of data minimization and inadequate technical and organizational measures to protect the data. The processor was also fined the equivalent of EUR 43,242.

To the fine notice of the UODO (dated 23 June 2025, in Polish)
To the press release of the UODO (dated 21 July 2025, in Polish)
To the notification on GDPRhub (dated 8 August 2025)

+++ SPAIN: EUR 250,000 FINE FOR UNAUTHORIZED COLLECTION OF FINGERPRINTS AND MISSING INFORMATION +++

The Spanish data protection authority Agencia Española de Protección de Datos (AEPD) has imposed a fine of EUR 250,000 on the zoo operator Loro Parque SA on Tenerife. Loro Parque had collected visitors' fingerprints when they purchased a combined ticket for entry to the zoo and the "Siam Park" water park. This was to ensure that the same visitor visited both parks. The park visitors were not informed about the data processing in advance. In addition, those park visitors who refused to give their fingerprints were denied entry. The AEPD found a violation of the general prohibition on the processing of sensitive data under Art. 9 (1) GDPR, which includes fingerprints as biometric data. In particular, there was no exception under Art. 9 (2) GDPR that would justify the processing. Even if the purchase of the combined ticket was voluntary, it was not possible to conclude that the park visitor had consented to the processing of their fingerprints solely on the basis of the purchase. Furthermore, Loro Parque had not carried out a data protection impact assessment prior to the processing. Loro Parque's appeal against the fine was unsuccessful.

To the AEPD's fine notice (dated 1 October 2024, in Spanish)

To the notification on GDPRhub (dated 6 August 2025)

+++ SPAIN: FINE OF EUR 200,000 AGAINST BANK FOR EXCESSIVE STORAGE +++

The Spanish data protection authority Agencia Española de Protección de Datos (AEPD) has imposed a fine of EUR 200,000 on Caixabank. This was prompted by a complaint from a private individual who had received mail to update a data protection policy of the bank without - according to his own statement - ever having concluded a contract with Caixabank. However, documents submitted by the bank referred to a contract concluded in 2005. The AEPD considered the storage of this data over such a long period of time to be a violation of Art. 5 (1) lit. e GDPR, according to which personal data may not be stored for longer than necessary. The authority rejected a request for reconsideration submitted by Caixabank.

To the decision of the AEPD (dated 5 June 2025, in Spanish)

To the AEPD's decision to reject the request for reconsideration (dated 19 August 2025, in Spanish)

To the notification on GDPRhub (dated 20 August 2025)

3. Opinions

+++ BFDI ON THE USE OF SOCIAL NETWORKS BY THE FEDERAL ADMINISTRATION +++

The German Federal Commissioner for Data Protection and Freedom of Information (BfDI) has issued guidance on the use of social networks by federal public bodies. This was triggered by the proceedings before the Administrative Court of Cologne, which allowed the Press and Information Office of the Federal Government to operate a Facebook fan page (see Privacy Ticker July 2025). The BfDI has now announced that it will appeal against the first instance ruling. The handout is intended to support public bodies in the lawful use of social networks until the issue of joint controllership has been clarified. The paper only explains the obligations arising from a public body's own responsibility as a fan page operator. This applies in particular to the content posted on the fan page. According to the guidelines, there must be a legal basis for data processing, the principles of transparency must be observed and, under certain circumstances, a data protection impact assessment must be carried out. In order to implement the principle of privacy by design, statistics functions and AI training with end user data, for example, should be deactivated. If required, the BfDI offers advice and exchange on the topic.

To the BfDI handout (dated 22 August 2025, in German)

To the BfDI press release (dated 22 August 2025, in German)

+++ EU COMMISSION USES MICROSOFT 365 IN COMPLIANCE WITH DATA PROTECTION LAW +++

In March 2024, the European Data Protection Supervisor (EDPS) identified the European Commission's use of Microsoft 365 in breach of data protection regulations (see Privacy Ticker March 2024). The Commission has now taken concrete compliance measures and thus ensured data protection-compliant use in the opinion of the EDPS. Among other things, the categories of personal data that are processed when using Microsoft 365 and the purposes of this processing have been specified. In an additional contractual agreement, Microsoft has undertaken to process the data only on documented instructions. It was also stipulated that third country transfers may only be made to selected recipients and for expressly defined purposes. Furthermore, the disclosure of personal data, e.g. to authorities, is only permitted if this is expressly provided for by EU law or the law of a member

state. Data may only be disclosed outside the EU on the basis of the law of the third country and if an appropriate level of protection is guaranteed. The Commission has implemented appropriate technical and organizational measures to ensure compliance with these precautions.

To the press release of the EDPS (dated 28 July 2025)

+++ BSI & ANSSI ON DESIGN PRINCIPLES FOR LLM-BASED SYSTEMS WITH ZERO TRUST +++

Together with the French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), the German Federal Office for Information Security (BSI) has published a position paper on design principles for LLM-based systems with Zero Trust. The proposed concepts serve as a basis for security measures during the development, planning, deployment and use of generative AI applications. The measures are intended to make LLM-based systems more resilient to hacking and other attacks and thus contribute to a trustworthy LLM system. The BSI and ANSSI name authentication and authorization for access to and use of an LLM system, restriction of input and output, sandboxing, monitoring, reporting and controlling as well as user awareness as key design principles. Specific implementation measures with brief explanations are also proposed for each of the design principles mentioned, such as two-factor authentication, memory management for sandboxing and practical awareness training for users.

To the BSI and ANSSI paper (from August 2025)

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: 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

Here you will find our complete imprint: www.advant-beiten.com/en/imprint and our privacy policy: www.advant-beiten.com/en/privacy-protection