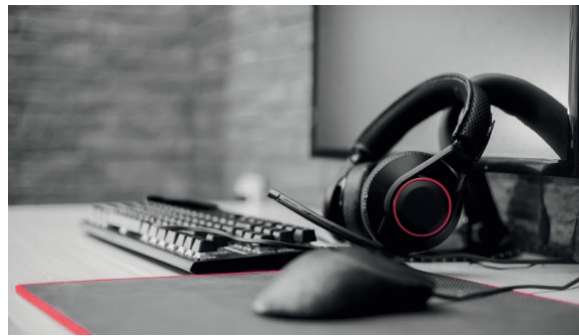


Privacy Ticker

February 2026



**+++ ACT FOR CRITICAL INFRASTRUCTURE PROTECTION PASSED
+++ FEDERAL COURT OF JUSTICE ON THE PERFORMANCE OF A
CONTRACT AS A LEGAL BASIS +++ ADEQUACY DECISION FOR
BRAZIL +++ FRANCE: EUR 5 MILLION FINE AGAINST STATE
EMPLOYMENT AGENCY +++ GOOGLE RECAPTCHA MOVES TO
ORDER PROCESSING +++**

1. Changes in Legislation

+++ ACT FOR CRITICAL INFRASTRUCTURE PROTECTION PASSED+++

The German Bundestag has passed the umbrella act for critical infrastructure protection, so called KRITIS law. The law serves to implement the EU Directive on the Resilience of Critical Facilities (CER Directive) and complements the IT security requirements ([NIS-2, see AB blog post of 29 January 2026](#)) to counter physical risks such as sabotage, terrorist attacks or natural disasters. The scope of application covers the following sectors: energy, transport and traffic, finance and insurance, health, drinking water, sewage, municipal waste disposal, information technology and telecommunications, food, space and public administration. Operators in these areas are obliged to carry out risk analyses, comply with minimum standards for the physical protection of critical infrastructures and report security incidents to a joint reporting office of the Federal Office of Civil Protection and Disaster Assistance and the Federal Office for Information Security. The regulations generally apply to facilities that supply more than 500,000 residents; violations can result in fines of up to EUR 1 million.

[To the press release of the Federal Government \(dated 29 January 2026, in German\)](#)

2. Case Law

+++ FEDERAL COURT OF JUSTICE ON THE PERFORMANCE OF A CONTRACT AS A LEGAL BASIS +++

The Federal Court of Justice has ruled that the transmission of e-mail addresses may be necessary for the performance of a contract within the meaning of Art. 6 (1) (b) GDPR. The background to this was an association dispute in which a member demanded the board of directors to hand over the e-mail addresses of the other members in order to contact them before a general meeting and to influence their voting behaviour on a certain topic. The board rejected this. The court clarifies that by joining the association, a contract is concluded, which is specified in the statutes. The enforcement of statutory membership rights, including the exertion of influence before a general meeting, was covered by this contract. The court holds that the transmission of the e-mail addresses of the members was the only way to exercise the statutory rights in connection with the decision-making process in the general assembly, and it is therefore covered by Art. 6 (1) (b) GDPR.

[To the ruling of the Federal Court of Justice \(dated 10 December 2025, II ZR 132/24, in German\)](#)

+++ REGIONAL COURT FRANKENTHAL: TESLA VIDEO ADMITTED AS EVIDENCE DESPITE POSSIBLE DATA PROTECTION VIOLATION+++

The Regional Court of Frankenthal (Palatinate) has clarified that video recordings of all-round cameras installed in vehicles ("guardian mode" of a Tesla) are admissible as evidence for the investigation of traffic accidents. In the underlying case, a car had driven into the open door of a parked Tesla. The person who caused the accident had claimed that the door of the Tesla had been suddenly opened immediately before the collision. He defended himself against the use of the camera recordings by invoking his right to informational self-determination. However, the court admitted the video, refuting the claim of the person who caused the accident that the door had suddenly opened. The court emphasizes that even a possible violation of data protection requirements does not automatically lead to a prohibition on the use of evidence in civil proceedings. In the context of the required balancing, the injured party's interest in providing evidence outweighs the data protection law of the other party in the accident. The ruling is not yet final.

[To the press release of the Regional Court of Frankenthal \(dated 7 July 2025, 5 O 4/25, in German\)](#)

+++ ADMINISTRATIVE COURT OF DÜSSELDORF: REDACTION OF THIRD-PARTY DATA PERMITTED IN THE CASE OF RIGHT TO INFORMATION +++

The Düsseldorf Administrative Court has dismissed a lawsuit for complete and unredacted data information. Although the controller had provided the data subject with information under data protection law as well as copies of the corresponding documents, he had blacked them out in part. The court confirms that the right to a copy of the data is limited exclusively to the personal data of the data subject. Therefore, a controller is entitled to make information unrelated to the data subject as well as personal data of third parties unrecognizable before handing over the copy. This applies, for example, to the names of government employees or reporting persons that are contained in the same files. The court holds that the right to information does not include the mandatory surrender of entire documents, but only the complete and faithful reproduction of one's own data. As long as these are not shortened or falsified by the redactions, the procedure is lawful. In the view of the court, there was no interest in bringing proceedings for further action for unredacted surrender anymore, since the right to information had already been fulfilled by the issue of the redacted copies.

[To the ruling of the Düsseldorf Administrative Court \(dated 28 January 2026, 29 K 9469/23, in German\)](#)

3. Regulatory Investigations and Enforcement Actions

+++ ADEQUACY DECISION FOR BRAZIL +++

The European Commission has adopted an adequacy decision for Brazil under Art. 45 GDPR. On this basis, personal data can now be transferred to the South American country without additional guarantees, such as the conclusion of standard contractual clauses. The basis for this is the European Commission's finding that the Brazilian legal framework and in particular the data protection law there guarantee a level of protection that is essentially equivalent to European standards. This also includes enforceable rights for data subjects as well as effective legal remedies against disproportionate access by national security authorities. Since Brazil has passed a corresponding decision for the European Union at the same time, this mutual recognition creates the world's largest area for free and secure data transfer, covering around 670 million consumers. The European Commission will evaluate the implementation and functioning of the adequacy decision every four years in the future.

[To the press release of the EU Commission \(dated 27 January 2026\)](#)

[To the EU Commission's implementing decision \(dated 27 January 2026\)](#)

+++ FRANCE: EUR 5 MILLION FINE AGAINST STATE EMPLOYMENT AGENCY +++

The French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) has imposed a fine of EUR 5 million on the state employment agency France Travail. The reason for this is a violation of the obligation to ensure the security of the processing of personal data (Art. 32 GDPR). In the first quarter of 2024, attackers had penetrated the facility's IT system, exposing the data of several million job seekers. The regulator's investigation uncovered several serious security vulnerabilities, including insufficiently robust authentication procedures, a lack of logging mechanisms to detect unusual behavior, and overly broad access permissions.

[To the CNIL press release \(dated 29 January 2026, in French\)](#)

[To the decision against France Travail \(dated 22 January 2026, in French\)](#)

+++ FRANCE: EUR 3.5 MILLION FINE FOR DATA TRANSFER TO SOCIAL NETWORK +++

The CNIL has also imposed a fine of EUR 3.5 million on a company that had transmitted customer data to a social network for advertising purposes without a legal basis. The regulator's investigation revealed that the company had shared email addresses and phone numbers of members of its loyalty program with the platform without first obtaining effective consent. The customers had not been informed that their data would flow to the social network, which is why the alleged consent could not be considered informed within the meaning of the GDPR. In addition, despite the large volume of data and the mass merging of data, the company had not carried out a data protection impact assessment in advance. Furthermore, the specifications for user passwords were not sufficiently secure and non-essential cookies were set without prior consent.

[To the CNIL press release \(dated 22 January 2026, in French\)](#)

[To the decision of the CNIL \(dated 30 December 2025, in French\)](#)

4. Opinions

+++ EDPB AND EDPS: JOINT OPINION ON THE DIGITAL OMNIBUS +++

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have published a joint opinion on the so-called "Digital Omnibus". After the EDPB and EDPS had already commented on the AI-specific aspects of the legislative package in an initial statement last month ([see Privacy Ticker January 2026](#)), they are now taking a general position on the planned regulatory simplifications. Both welcome the European Union's fundamental plan to simplify regulatory requirements in the digital sector, reduce administrative burdens and strengthen competitiveness. At the same time, however, they express key concerns about the concrete implementation and warn in particular that the change in the definition of personal data in the GDPR envisaged in the draft goes far beyond a mere technical adjustment. Even if approaches to combat the so-called cookie banner fatigue within the framework of the ePrivacy Directive are expressly welcomed, a general reduction in bureaucratic burdens should not be at the expense of informational self-determination and the fundamental rights of the data subjects.

[To the press release of the EDPS \(dated 11 February 2026\)](#)

+++ EDPB: RESULTS OF THE AUDIT ACTION ON THE RIGHT TO ERASURE PUBLISHED +++

The European Data Protection Board (EDPB) has published the final report on its coordinated audit action of the past year ([see Privacy Ticker March 2025](#)). The focus of the Europe-wide investigations was on the practical implementation of the right to erasure under Art. 17 GDPR. The evaluation of the national investigations has shown that there is still considerable room for improvement among many controllers. The supervisory authorities have identified a total of seven recurring challenges. In practice, there is often a lack of suitable internal procedures for processing deletion requests or for sufficient deletion through anonymization. In addition, the necessary balancing of interests in the application of exceptions causes difficulties for many companies, as the right to erasure does not apply without restriction. For the current year, the EDPB has already defined the focus of the new audit action: Within the so-called Coordinated Enforcement Framework 2026, the supervisory authorities will focus on compliance with the transparency and information obligations under Articles 12 to 14 GDPR.

[To the EDPB's press release \(dated 18 February 2026\)](#)

+++ GOOGLE RECAPTCHA MOVES TO ORDER PROCESSING +++

Google has made far-reaching changes to its bot protection service reCAPTCHA to make it more privacy-friendly. As media report, Google will no longer act as an independent controller in the analysis of user behavior in the future, but as a pure processor. So far, Google itself has decided how and for what purposes the information collected in the background is processed. In response to the steadily growing regulatory pressure in Europe, data sovereignty will be transferred in full to the operators of the respective websites from April 2026, who will thus also be responsible for the processing of the data collected on their websites in this respect.

[To the report by heise online \(dated 8 February 2026\)](#)

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](#)



Office Hamburg

Neuer Wall 72 | 20354 Hamburg

Jan-Dierk Schaal

+49 40 688745-0

[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

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