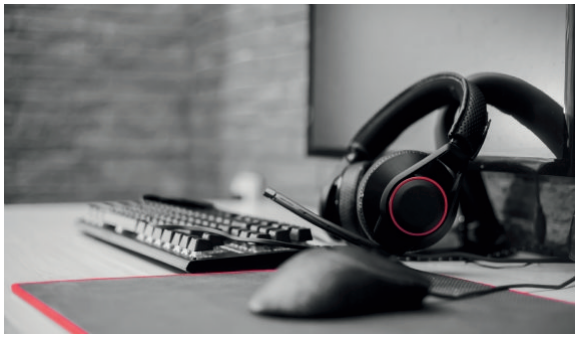
ADVANT Beiten

Privacy Ticker

April 2026



+++ FEDERAL COURT OF JUSTICE: RIGHT TO INFORMATION CANNOT BE ASSERTED AS A DERIVATIVE RIGHT BY THIRD PARTIES +++ ADMINISTRATIVE COURT OF DÜSSELDORF: TRANSPORT ENCRYPTION FOR E-MAILS IS GENERALLY SUFFICIENT +++ ITALY: FINE OF EUR 31.8 MILLION AGAINST BANK FOR UNAUTHORISED ACCESS TO CUSTOMER DATA +++ EDPB PUBLISHES DPIA TEMPLATE +++ FEDERAL COUNCIL: STATEMENT ON DATA PROTECTION REGULATIONS IN THE "DIGITAL OMNIBUS" +++

1. Case Law

+++ FEDERAL COURT OF JUSTICE: RIGHT TO INFORMATION CANNOT BE ASSERTED AS A DERIVATIVE RIGHT BY THIRD PARTIES +++

The Federal Court of Justice has ruled on the assertion of the right to information based on an assigned claim and by third parties. The plaintiff had consumers assign claims against their insurance company by way of the purchase of receivables in order to assert them in its own name. Only claims for reimbursement and damages were expressly assigned. For claims to information, there was only a power of attorney to assert them. The plaintiff demanded information from the insurance company in accordance with Art. 15 GDPR, which the Court ultimately denied. On the one hand, the Court found that the right to information had not been assigned in the specific case itself. The claim is also not merely an ancillary or auxiliary right to the claims for reimbursement and damages and therefore does not automatically transfer with them. On the other hand, the plaintiff was also not entitled by the power of attorney to assert

the insured person’s claims for information in her own name.

To the ruling of the Federal Court of Justice (dated 24 February 2026, VI ZR 430/24, in German)

+++ ADMINISTRATIVE COURT OF DÜSSELDORF: TRANSPORT ENCRYPTION FOR E-MAILS IS GENERALLY SUFFICIENT +++

The Administrative Court of Düsseldorf has determined that transport encryption is sufficient when sending data with normal risk. End-to-end encryption is not necessary in these cases. For the plaintiff, a restriction on the disclosure of information had been entered in the population register. In connection with a bus accident, the bus company transmitted the plaintiff's name and information about the accident to the liability insurance company by e-mail using transport encryption. After an unsuccessful complaint to the data protection authority, the plaintiff filed a lawsuit to oblige the authority to intervene against the bus company. The court did not see a data protection violation here and found that the data transmitted by e-mail was not particularly sensitive and that transport encryption was therefore an adequate protection. Despite the restriction on the disclosure of information registered for the plaintiff, there was no increased risk.

To the ruling of the Düsseldorf Administrative Court (dated 2 April 2026, 29 K 7351/23, in German)

+++ REGIONAL COURT OF KREFELD: NO COMPENSATION FOR ZERO-DAY EXPLOIT +++

The Regional Court of Krefeld has ruled that a company is only liable in the event of a cyber attack if it can be proven to be culpable. In the case, the defendant insurance company had been the victim of a hacker attack in which personal data of customers was affected. In the attack, the perpetrators used a security vulnerability previously unknown to the software manufacturer (so-called zero-day exploit). The court dismissed the action of a data subject because it could not be established that the company was at fault. Rather, the defendant had used commercially available and certified software, and the security vulnerability had not been known beforehand. Since the GDPR does not require absolute protection, the technical and organizational measures were sufficient. The court clarified that a successful cyber attack alone is not a reliable indication of inadequate technical and organizational measures.

To the ruling of the Regional Court of Krefeld (dated 6 November 2025, 3 O 93/24, in German)

2. Regulatory Investigations and Enforcement Actions

+++ ITALY: FINE OF EUR 31.8 MILLION AGAINST BANK FOR UNAUTHORIZED ACCESS TO CUSTOMER DATA +++

The Italian data protection authority Garante per la Protezione dei Dati Personali (GPDP) has imposed a fine of EUR 31.8 million on the bank Intesa Sanpaolo S.p.A. After the bank reported a data breach, the authority found serious deficiencies in the implemented technical and organizational measures. For example, an employee had unlawful access to the bank details of 3,573 customers for about two years and repeatedly called them up. These inadmissible accesses were not detected by the internal control systems. The illegal access also affected data on "high-risk" customers, including persons with public functions, for whom increased control measures would have been necessary. In addition, the report of the data breach by the bank was incomplete and late. A notification to the affected persons was only made after request by the GPDP.

To the press release of the GPDP (dated 30 March 2026, in Italian)

To the fine notice of the GPDP (dated 26 March 2026, in Italian)

+++ ITALY: FINE OF EUR 17.6 MILLION AGAINST BANK FOR PASSING ON CUSTOMER DATA +++

The Italian data protection authority GPDP has imposed a further fine of EUR 17.6 million on the aforementioned bank Intesa Sanpaolo S.p.A. The bank had transmitted the data of about 2.4 million customers to its subsidiary Isybank S.p.A. In order to identify which customers were to be transferred to the newly founded Isybank, Intesa Sanpaolo carried out a profiling of its customers without a legal basis and illegally transmitted the data to Isybank. In addition, the authority found that the customers had not been sufficiently informed about the events. For example, the corresponding notifications had been sent during the summer period and stored in the archive area of the bank's app without separately informing customers of the data processing.

To the press release of the GPDP (dated 12 March 2026, in Italian)

To the fine notice of the GPDP (dated 12 March 2026, in Italian)

+++ SPAIN: FINE OF EUR 950,000 FOR INADMISSIBLE PROCESSING OF BIOMETRIC DATA +++

The Spanish data protection authority Agencia Española de Protección de Datos (AEPD) has imposed a fine of EUR 950,000 on the British company YOTI Ltd. YOTI specializes in identity and age verification and operates an app that is used for age verification. In the app, users' identity documents and selfies were processed to create a biometric face template. The authority came to the conclusion that the biometric data of the users was processed without a legal basis. A consent obtained by YOTI was invalid because it was too general, and the checkbox was pre-ticked. In addition, users' data, in particular biometric data, geolocation data, verification videos and identity documents, were stored for longer than necessary. The authority assessed the fact that the app was largely aimed at minors as an aggravating factor.

To the AEPD's fine notice (dated 10 March 2026, in Spanish)

3. Opinions

+++ EDPB PUBLISHES DPIA TEMPLATE +++

The European Data Protection Board (EDPB) has published a template and accompanying guidance for data protection impact assessments (DPIA) in accordance with Art. 35 GDPR. The template is intended to support controllers in conducting and documenting DPIA checks. It is a consequence of the so-called Helsinki Statement, in which the European data protection supervisory authorities agreed to develop practical and understandable tools, especially for small and medium-sized organizations, to implement the risk-based approach of the GDPR. Interested parties can comment on the draft in a public consultation until 9 June 2026. Subsequently, it is planned that the supervisory authorities will either adopt the template as a standard or develop country-specific templates on the basis of it.

To the DPIA submission (dated 10 March 2026)

To the instructions for the DPIA template (dated 10 March 2026)

+++ FEDERAL COUNCIL: STATEMENT ON DATA PROTECTION REGULATIONS IN THE "DIGITAL OMNIBUS" +++

The Federal Council comments on the planned amendments of the Digital Omnibus Regulation in the area of data protection law. In doing so, it welcomes the proposals of the EU Commission, but sees a need for further adaptation and submits specific proposals. For example, the right to information under Art. 15 GDPR may only be asserted once every two years free of charge. In addition, data that the data subject has provided themselves is to be excluded. The scope of application of Art. 9 GDPR is to be limited to the effect that processing only includes special categories of personal data if the processing is intended to derive such categories of data. In addition, Art. 9 GDPR is to be supplemented by a new basis for the performance of a contract or for the implementation of pre-contractual measures. In the case of autonomous driving systems, the Federal Council opposes a consent requirement and advocates simplifying the processing of image and video data.

To the decision of the Federal Council (dated 27 March 2026, in German)

+++ EDPB: GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR SCIENTIFIC RESEARCH PURPOSES +++

The EDPB has published guidelines on the processing of personal data for scientific research purposes. Among other things, it presents six key indicators on the nature, scope, context and purposes of the processing, which serve to classify whether research is considered "scientific" within the meaning of the GDPR. In the EDPB's view, further processing for scientific purposes should in principle be considered compatible with the original purpose, without the need for a purpose compatibility test. Longer storage of data should be permitted if this is necessary for future research projects. For (still) undetermined research purposes, broad or dynamic consent can serve as an appropriate legal basis, with additional safeguards required. In addition, the EDPB explains the conditions under which rights such as erasure and objection can be restricted. Overall, the EDPB stresses the importance of ethical standards and technical measures to protect the rights and freedoms of data subjects.

To the EDPB Guidelines 1/2026 (dated 15 April 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

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