View in browser


Privacy, Cybersecurity, and Data Innovation Update

April 17, 2026

# European Data Privacy Newsletter

We are pleased to provide you with the March 2026 edition of Gibson Dunn's monthly European privacy, cybersecurity, and data innovation update. Please feel free to reach out to us to discuss any of the below topics further.

## Europe

03/26/2026

### EDPB | Report | Legitimate Interest

**The European Data Protection Board (EDPB) provides practical enforcement insight into how supervisory authorities assess reliance on legitimate interest under the GDPR.**

This thematic digest compiles and analyses one-stop-shop decisions from the EDPB register, showing how supervisory authorities apply the three-step test under Article 6(1)(f) of the GDPR in different factual scenarios. The report includes compliant and non-compliant examples, reflects recent guidance, and refers to relevant EU case law and national decisions. It is intended as a practical tool for authorities and controllers by clarifying how necessity and balancing tests are assessed in enforcement practice.

For more information: EDPB Commissioned Report

03/26/2026

## ENISA | Guidance | Cybersecurity Market Analysis Framework

**The European Union Agency for Cybersecurity (ENISA) updated its guidance on how to conduct market analysis in the field of cybersecurity.**

This new version of the ENISA Cybersecurity Market Analysis Framework incorporates lessons learned from previous applications. It strengthens the framework's ability to respond to both immediate policy needs and long-term monitoring requirements while aligning with recent EU legislation such as the NIS 2 Directive and the Cyber Resilience Act.

For more information: ENISA Cybersecurity Market Analysis Framework

03/19/2026

## EDPB | GDPR | Transparency

**The European Data Protection Board (EDPB) launches coordinated enforcement action on transparency and information obligations under the GDPR.**

On March 19, the EDPB launched its 2026 Coordinated Enforcement Framework CEF action, shifting focus from the 2025 right-to-erasure work to GDPR transparency and information obligations. In 2026, 25 European data protection authorities will review how organizations inform individuals about data processing, using enforcement and fact-finding across sectors. Findings will be pooled in the second half of the year, culminating in an EDPB report to guide follow-up at both national and EU levels.

For more information: EDPB Website

03/19/2026

## CJEU | Judgment | GDPR Access Request

**The European Court of Justice (CJEU) clarifies that a GDPR access request may be considered abusive and refused.**

In its judgment in Case C-526/24, the EU Court of Justice held that even a first GDPR access request made under Article 15 of the GDPR can be refused as "excessive" or abusive where it's made solely to manufacture a compensation claim.

Controllers may rely on patterns of repeated requests and litigation to demonstrate abusive intent. The Court also confirmed that compensation under the GDPR requires proof of actual material or non-material damage and cannot be granted where the data subject's own conduct is the determining cause of the harm.

For more information: CJEU Website

03/18/2026

## EDPB-EDPS | Joint Opinion | Cybersecurity Act 2 and NIS 2

**The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) adopted a joint opinion on proposals for a Cybersecurity Act 2 (CSA2) and amendments to the NIS 2 Directive.**

The EDPB and EDPS support the CSA2 and NIS2 proposals to strengthen ENISA's role, facilitate cybersecurity certification, and address ICT supply chain risks, including the non-technical ones. In addition, the EDPB and EDPS strongly support the establishment of a single-entry point for the notification of personal data breaches.

For more information: EDPB Website

03/12/2026

## EDPB-EDPS | Joint Opinion | European Biotech Act and Clinical Trials

**The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) support the European Commission's proposal for a European Biotech Act to harmonize clinical trials across the EU, while insisting on robust, purpose-specific safeguards to protect sensitive health and genetic data.**

In their Joint Opinion, the EDPB and EDPS welcome the introduction of a single legal basis for the processing of personal data by sponsors and investigators under the Clinical Trials Regulation, as a means to reduce fragmentation and increase legal certainty. At the same time, they stress that simplification must not lower data protection standards and recommend targeted safeguards, including clearer controller roles, limits on data retention, strict conditions for further processing, coherence with the AI Act, and the use of appropriate technical and organizational measures such as pseudonymization.

For more information: EDPB Website

03/04/2026

### EDPB | Study | Data Brokers

**The EDPB has released a new study mapping the data-broker market and identifying high-risk personal data providers and intermediaries.**

The EDPB's Data Brokers Market Study, completed in November 2025 at the request of the Belgian DPA, provides a methodology for identifying data brokers and assesses their business models and associated risks. Focused on the Belgian market, the study reveals a highly diverse landscape of data brokers and providers with varying levels of risk related to personal data use. Beyond its national scope, the report offers a broader framework to help detect high-risk data brokers across Europe.

For more information: EDPB Website

---

## France

03/20/2026

### CNIL | Guidance | Sound Recording

**The French Supervisory Authority (CNIL) reiterated that sound recording is generally prohibited in video surveillance systems.**

The CNIL confirms that audio capture integrated into video surveillance is banned due to significant risks to privacy and freedom of expression. However, standalone audio recording systems may be permitted in limited cases, provided they are not automatically linked to cameras and are triggered manually (e.g. in case of aggression). Such systems must remain exceptional, necessary, and proportionate, with strict safeguards on activation, retention (only in case of incidents), staff training, and transparency toward individuals.

For more information: CNIL Website [FR]

03/10/2026

## CNIL | Guidance | Data Governance Act

**The French Supervisory Authority (CNIL) published guidance on Data Altruism Organizations (DAOs) under the EU Data Governance Act.**

DAOs enable voluntary data sharing for general interest purposes and must meet specific requirements, including non-profit status, legal independence from for-profit entities, and transparent governance. The CNIL serves as France's competent authority for DAO registration and clarifies key operational questions, including permissible legal forms, subcontracting rules, and how DAOs may receive fees or provide compensation to data holders.

For more information: CNIL Website [FR]

03/04/2026

## French Council of State | Judgment | GDPR

**The French Council of State (Conseil d'État) upheld the French supervisory authority (CNIL) €40 million fine against an adtech company for GDPR violations related to its targeted advertising practices.**

The court considered that the company failed to demonstrate valid user consent for data processing, provided inadequate transparency about its data use purposes (including algorithm training), and did not properly erase data when users withdrew consent. Notably, the ruling reaffirms that pseudonymized cookie identifiers linked to browsing data, IP addresses, and purchase history constitute personal data under the GDPR, as re-identification remains technically feasible without disproportionate effort.

For more information: Conseil d'État Website [FR]

03/02/2026

### CNIL | Caselaw Compilation | 2026 Data Protection Caselaw Table

**The French Supervisory Authority (CNIL) has released its 2026 update to the "Tables Informatique et Libertés," a reference document compiling key case law and regulatory decisions on personal data protection.**

Designed for legal professionals and academics, the tables summarize rulings from the CNIL, the CJEU, the ECtHR, French courts, and the EDPB, organized by theme (principles, legal bases, individual rights, security, transfers, and sanctions). The publication aims to promote consistency in the CNIL's enforcement practices while increasing transparency around its legal reasoning.

For more information: CNIL Website [FR]

---

## Germany

03/26/2026

### German Parliament | Legislation | EU Data Act and Data Governance Act

**Germany has adopted two laws implementing the Data Act and the Data Governance Act.**

The two implementing laws establish national rules on supervision, procedures and sanctions for the enforcement of both EU instruments. The Federal Network Agency (Bundesnetzagentur) has been designated as the competent authority for enforcing both the Data Act and the Data Governance Act, while the Federal Statistical Office will act as the central information point and provide support to public bodies in connection with decisions on the reuse of protected public-sector data under the Data Governance Act. The new national measures also introduce administrative fines of up to €500,000.

For more information: German Parliament Website [DE]

03/25/2026

## Hamburg Supervisory Authority | Report | 2025 Data Protection Activity

**Hamburg Supervisory Authority (HmbBfDI) has published its 2025 report, highlighting a significant increase in complaints and the role of AI in this development.**

The report records over 4,200 complaints, representing an increase of 60% compared to 2024, and observes that this upward trend has continued into 2026. It points to growing public dissatisfaction with digital services, particularly social networks, where complaint volumes have nearly tripled. According to the authority, the increasing use of AI has contributed to this trend in two ways. On the one hand, individuals are making growing use of AI tools to assist them in submitting complaints. On the other hand, the deployment of insufficiently mature AI systems is negatively affecting digital customer service and giving rise to data protection concerns.

For more information: HmbBfDI Website [DE]

03/06/2026

## Federal Administrative Court | Judgment | Health Data and Preventive Programs

**Germany's Federal Administrative Court (BVerwG) has held that private health insurers may not, without consent, analyze diagnoses contained in reimbursement invoices to identify potential participants for preventive programs.**

The Court held that the insurer's practice did not breach Article 9(1) GDPR because the health-prevention derogation in Article 9(2)(h) GDPR could in principle apply, and Section 22(1) no. 1(b) BDSG provided the necessary national-law basis. It nevertheless found the processing unlawful because it could not be justified under Article 6(1)(f) GDPR. In the Court's view, the insured persons' interests prevailed in the balancing exercise, given the heightened protection of health data under Article 9, the fact that the programs were outside the medical core area, the broad scope of the analysis, and the insurer's failure to explain its interests clearly enough to data subjects. The Court left open whether the re-use of the data also infringed the purpose-limitation principle.

For more information: Federal Administrative Court Website [DE]

# Spain

03/25/2026

### Spanish Supervisory Authority | Strategy | 2026 Action Plan and 2025 Implementation Report

**The Spanish Supervisory Authority (AEPD) published a near-complete 2025 scorecard and a 2026 action plan with a heavier emphasis on privacy technology and AI.**

The AEPD says five of the seven strategic axes from 2025 were completed at 100%, while the other two exceeded 97%, with overall execution above 99%. Its 2026 plan sets 32 operational objectives and 115 actions, including privacy-lab work, technological experimentation, AI tools and automation.

For more information: AEPD Website [ES]

03/24/2026

### Spanish Supervisory Authority | Guidance | Personal Data Breaches

**The Spanish Supervisory Authority (AEPD) refreshed its operational guidance on how organizations should notify personal data breaches, reinforcing Article 33 compliance expectations.**

The AEPD updated its guidance page on notifying personal data breaches to the supervisory authority, reiterating that breach notifications should be submitted electronically via the designated e-filing process and that notifying a breach does not automatically mean an investigation will follow. The page restates core GDPR framing: timely notification is part of accountability, failure to notify where required is an infringement, and controllers must document breaches even where they assess no risk to individuals' rights and freedoms. This is a practical reference for incident response playbooks, particularly for multinational teams coordinating EU breach notifications.

For more information: AEPD Website [ES]

03/04/2026

### National Cryptologic Center | Infographics | NIS2 Compliance

**Spain's National Cryptologic Center (CNN) has published four infographics to help entities navigate NIS2 compliance.**
The materials cover the Directive's key points, core requirements, scope, and a practical compliance guide, and stress that ENS Certificates of Conformity can be used to support demonstration of NIS2 compliance. The initiative builds on the CCN's wider work aligning ENS tools with NIS2 requirements and gives organizations a short operational reference for scoping obligations and evidencing baseline cybersecurity governance.

For more information: CCN Website [ES]

03/04/2026

### Spanish Supervisory Authority | Sanction | Data Protection Impact Assessment

**The Spanish Supervisory Authority (AEPD) fined a football club €500,000 for rolling out biometric identity checks for members without a compliant prior DPIA.**

The case concerns the club's 2023 digital census update, which used facial biometrics and optional voice biometrics for member verification. According to the published reporting on the decision, the AEPD found that the scale of the processing, the use of biometrics, the involvement of minors and the potential legal impact for members required a full Article 35 GDPR assessment before deployment, and that the club's internal risk documentation did not meet that standard.

For more information: AEPD Resolution [ES]

---

## United Kingdom

03/31/2026

### ICO | Report | Use of Automated Decision Making in Recruitment

**The UK Supervisory Authority (ICO) has published a report highlighting risks and regulatory expectations for the use of automated decision-making (ADM) in recruitment.**

The report identifies concerns around lack of transparency, insufficient human involvement, misuse of automated tools, and risks of bias or discrimination in relation to ADM in recruitment. It stresses that employers must assess whether recruitment decisions are solely automated, apply the safeguards required under UK GDPR, provide clear information to candidates, ensure genuine human review where ADM is relied on, and carry out robust DPIAs for high-risk processing.

For more information: ICO Website and Report

03/26/2026

## ICO | Sanction | Company Fined £100,000 for Unlawful Direct Marketing Calls

**The UK Supervisory Authority (ICO) sanctioned a UK company for large-scale unlawful telemarketing targeting vulnerable individuals.**

The ICO issued a fine of £100,000 (€115,447) after a company made over 260,000 unsolicited marketing calls to individuals registered with the Telephone Preference Service, in breach of Privacy and Electronic Communications Regulations (PECR) requirements. Investigations revealed misleading practices, including false caller identities and targeting of older individuals, as well as the use of unlawfully obtained third-party data. The enforcement action, issued under the Data Protection Act 1998 and PECR, underscores the regulator's continued focus on intrusive direct marketing and the importance of consent, transparency and lawful data sourcing.

For more information: ICO Website

03/25/2026

## ICO-Ofcom | Joint Statement | Age Assurance

**The UK Supervisory Authority (ICO) and the UK's regulator for communications services (Ofcom) aligned their age-assurance expectations and reiterated that self-declaration alone is not enough.**

The joint statement is aimed at child-accessed services subject to both the Online Safety Act and UK data protection law (UK GDPR and Data Protection Act 2018), and presents a risk-based, tech-neutral approach to age assurance. It states that age assurance must be effective, necessary, and proportionate, notes that self-declaration alone is not an effective means of preventing underage access, and links robust age gates to avoiding unlawful processing of children's data.

For more information: ICO Website

03/02/2026

## UK Government I Public Consultation I Online Child Safety

**The UK Government opened a consultation on online child safety and AI chatbots.**

The consultation has five chapters covering how children use technology, possible intervention strategies, approaches to enforcement and compliance, preparing children for a digital future and supporting families. The consultation includes several questions on AI chatbots and social media, including whether such offerings should be subject to minimum age restrictions, and whether the digital age of consent should be raised. The consultation is open until 26 May.

For more information: Government Website

**The following Gibson Dunn lawyers prepared this update: Ahmed Baladi, Vera Lukic, Kai Gesing, Joel Harrison, Thomas Baculard, Ioana Burtea, Billur Cinar, Hermine Hubert, Christoph Jacob, Yannick Oberacker, and Phoebe Rowson-Stevens.**

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

**Privacy, Cybersecurity, and Data Innovation**:

**United States**:
Abbey A. Barrera – San Francisco (+1 415.393.8262, abarrera@gibsondunn.com)
Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com)
Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com)
Lauren R. Goldman – New York (+1 212.351.2375, lgoldman@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Natalie J. Hausknecht – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com)
Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Martie Kutscher Clark – Palo Alto (+1 650.849.5348, mkutscherclark@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com)
Frances A. Waldmann – Los Angeles (+1 213.229.7914,fwaldmann@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com)

**Europe**:
Ahmed Baladi – Paris (+33 1 56 43 13 00, abaladi@gibsondunn.com)
Patrick Doris – London (+44 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com)
Lore Leitner – London (+44 20 7071 4987, lleitner@gibsondunn.com)
Vera Lukic – Paris (+33 1 56 43 13 00, vlukic@gibsondunn.com)
Lars Petersen – Frankfurt/Riyadh (+49 69 247 411 525, lpetersen@gibsondunn.com)
Christian Riis-Madsen – Brussels (+32 2 554 72 05, criis@gibsondunn.com)
Robert Spano – London/Paris (+44 20 7071 4000, rspano@gibsondunn.com)

**Asia**:
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)