View in browser

Privacy, Cybersecurity, and Data Innovation Update

17 March 2026

European Data Privacy Newsletter

We are pleased to provide you with the February 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

02/23/2026

EDPB-EDPS | Joint Statement | AI-Generated Imagery and Privacy

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) signed a joint statement on AI-generated imagery and the protection of privacy.

The statement, endorsed by 61 data protection authorities worldwide, raises concerns about AI tools that create highly realistic images and videos of individuals without their knowledge or consent. It calls on organisations to ensure full compliance with data protection laws, implement strong safeguards and transparency measures, and engage proactively with regulators to prevent potential harm.

For more information: EDPB Website

02/18/2026

EDPB | Coordinated Enforcement Framework | Report on the Right to be Forgotten

The European Data Protection Board's (EDPB) has adopted a report under its Coordinated Enforcement Framework (CEF) action on the right to be forgotten.

The report highlights good practices identified across organizations, as well as recurring challenges they face when implementing the right to be forgotten. Among these challenges, the report particularly notes the lack of appropriate internal procedures, reliance on ineffective anonymization techniques, and difficulties in determining appropriate data retention periods.

For more information: EDPB Website

02/13/2026

EDPB | Policy | 2026-2027 Work Program

The European Data Protection Board's (EDPB) has adopted its work program for 2026-2027, placing an emphasis on "easing compliance" for organizations.

To simplify GDPR compliance, the EDPB will develop ready-to-use templates for organizations, including models for legitimate interest assessments, records of processing activities, privacy notices, data breach notifications, and data protection impact assessments.

For more information: EDPB Press Release

02/13/2026

European Commission | Toolbox | ICT Supply Chain Security

The European Commission has introduced a new ICT Supply Chain Security Toolbox aimed at reducing systemic dependencies and mitigate supplier-related risks.

The toolbox defines key concepts, outlines major risk scenarios and proposes mitigation measures, including enhanced risk-management practices and the adoption of multi-vendor strategies. This initiative forms part of the Commission's broader cybersecurity agenda, which also includes the proposed revision of the Cybersecurity Act presented in January 2026.

For more information: European Commission Website

02/11/2026

EDPB-EDPS | Joint Opinion | Digital Omnibus Regulation Proposal

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have published a joint opinion on the Digital Omnibus Regulation Proposal.

They welcome targeted amendments to the GDPR intended to reduce administrative burden and enhance legal certainty (e.g., new derogation allowing the processing of sensitive data for biometric authentication; introduction of EU-wide templates for data breach notifications and data protection impact assessments). However, the EDPB and EDPS strongly oppose proposals to redefine "personal data" or to empower the Commission, via implementing acts, to determine when pseudonymized data "is no longer personal." They warn that such changes would narrow the scope of the GDPR and risk undermining fundamental rights.

For more information: EDPB Website

02/02/2026

European Parliament | Opinion | AI Act Omnibus

The Committee of Legal Affairs of the European Parliament proposed substantial changes to the AI Act, tightening safeguards, expanding prohibited practices, and revising enforcement, governance and timelines.

On February 2, 2026, the Committee of Legal Affairs of the European Parliament issued a draft opinion on the AI Omnibus legislative proposal. The proposed amendments seek to explicitly cover agentic AI by extending the definition of AI systems to include systems that execute autonomous actions and proposes stricter

rules for processing special-category data for bias detection by requiring it to be “strictly necessary.” It also suggests adding a new prohibited practice covering AI systems that generate or manipulate sexualized content.

On governance, the draft opinion seeks to remove broad real-world testing outside sandboxes, and align cybersecurity compliance with the Cyber Resilience Act. It also replaces the flexible entry-into-force mechanism with fixed dates, with high-risk obligations applying from December 2027 and 2028, and legacy systems to be compliant by the end of 2030.

For more information: Draft Opinion of the Committee on Legal Affairs

---

France

02/26/2026

CNIL | GDPR | AI models

PANAME Project: French authorities seek Testers for New AI Privacy Audit Tool.

The French supervisory authority (CNIL), alongside other French agencies including ANSSI, PEReN, and Inria, has launched a call for interest inviting organizations to test PANAME, an open-source software library designed to audit AI models for GDPR compliance. The tool enables users to conduct data extraction and re-identification tests to assess whether AI models trained on personal data meet privacy requirements. Public and private entities established in EU member states are eligible to participate in this testing phase. Applications are open from February 26 through March 28, 2026.

For more information: CNIL Website [FR]

02/25/2026

CNIL | Public Consultation | Recommendation on Session Replay Tools

The French supervisory authority (CNIL) opened public consultation on its draft recommendations on session replay tools.

The CNIL has launched a public consultation on draft recommendations governing session replay tools (i.e., technologies that record and reconstruct users' complete browsing sessions on websites and mobile apps, including mouse movements, clicks, scrolling, and form inputs). The guidance targets both tool providers and website or app publishers, addressing key GDPR requirements such as data minimization and user consent mechanisms. Stakeholders are invited to submit comments by April 22, 2026.

For more information: CNIL Website [FR]

02/18/2026

DGFiP | Data Breach | Illegal access to the national bank accounts registers

FICOBA data breach exposed 1.2 million French bank accounts.

France's General Directorate of Public Finances (DGFiP) has disclosed a data breach affecting approximately 1.2 million bank accounts in the national bank account registry (FICOBA) after a malicious actor gained access using stolen government credentials in late January 2026. Compromised data includes bank account details (RIB/IBAN), account holder identities, and addresses, though tax identification numbers were not accessed. Authorities have implemented immediate access restrictions, notified the French Supervisory Authority (CNIL), filed a criminal complaint, and are coordinating with French cybersecurity agency (ANSSI) and banking institutions. Affected individuals will receive direct notifications, and users are urged to remain vigilant against phishing attempts.

For more information: DGFiP Press Release [FR]

02/18/2026

CNIL | GDPR | Right to erasure

The French supervisory authority (CNIL) released findings from coordinated European right to erasure inspections.

As part of a coordinated enforcement action led by the European Data Protection Board (EDPB), the CNIL conducted on-site inspections of six organizations in 2025 to assess compliance with GDPR right to erasure requirements. While data controllers generally honored deletion requests, inspectors identified persistent issues including inadequate internal procedures, insufficient information provided to data subjects, and difficulties determining data retention periods. Larger organizations demonstrated higher compliance levels and more formalized processes. The CNIL has already issued two formal notices, with additional corrective measures potentially forthcoming.

For more information: CNIL Website [FR]

02/13/2026

French Council of State | Judgment | Pseudonymization

French Council of State (Conseil d'État) upheld €1.8 million in French supervisory authority (CNIL) fines against health data companies.

The French Council of State (Conseil d'État) has rejected appeals by health data group companies challenging CNIL fines totaling €1.8 million for unlawfully processing health data collected from physicians and pharmacies. The French court confirmed that the companies' pseudonymized databases, containing data on millions of patients, constituted personal data under GDPR because re-identification remained possible using reasonable means. The ruling upheld CNIL's position that such health data processing requires prior authorization under French law, and that pseudonymization alone does not render data anonymous or exempt from GDPR requirements.

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

02/09/2026

CNIL | Report | 2025 Enforcement Actions

The French supervisory authority (CNIL) reported record €487 million in fines for 2025.

The CNIL issued 83 sanctions totaling €486.8 million in 2025, with cookies, employee video surveillance, and data security violations among the top enforcement priorities. Two major fines of €325 million and €150 million were imposed for cookie consent violations, while 16 organizations were sanctioned for unlawfully surveilling employees. Other recurring issues included inadequate data security measures, failure to cooperate with the CNIL, and non-compliance with data subject rights such as erasure and access requests. The CNIL also issued 143 formal notices, notably targeting child welfare services and mobile apps used by minors.

For more information: CNIL Website [FR]

Germany

02/26/2026

Data Protection Conference (DSK) | Statement | "Chat Control"

The German Data Protection Conference (DSK) called for a complete rejection of proposals that would require indiscriminate scanning of private digital communications (Chat Control).

Ahead of EU negotiations, the DSK urged policymakers to abandon mass surveillance of private chats, bulk scanning of messages and any weakening of end-to-end encryption, while emphasizing that child-protection measures must remain targeted and proportionate; it also pointed to Article 28 of the Digital Services Act as already requiring platforms accessible to minors to adopt appropriate safeguards.

For more information: DSK Website [DE]

02/25/2026

Data Protection Authority North Rhine-Westphalia | Survey | Centralized Data Protection Supervision

The Data Protection Authority North Rhine-Westphalia cited a new Bitkom survey to argue against proposals to centralise private-sector data protection supervision at the federal level.

According to the authority, the survey of 603 companies found that 85% want clearer data protection rules, 79% call for GDPR reform and 69% want better alignment with other regulatory frameworks, while 62% are asking supervisory authorities for more practical guidance; the authority also said complaints in NRW rose by 67% last year and noted that only 9% of respondents saw no disadvantages in a shift to federal-level supervision.

For more information: LDI NRW Website [DE]

02/12/2026

Data Protection Conference (DSK) | Statement | Draft Research Data Act (FDG)

The German Data Protection Conference (DSK) welcomed the goal of improving access to research data but said the draft Research Data Act (FDG) requires substantial revision.

In its statement, the DSK called for clearer delineation between the FDG and sector-specific research laws, particularly for health data, stronger independence and separation safeguards for the proposed German Center for Microdata, a clearer allocation of controller responsibilities, more precise limits on data access and retention, mandatory data protection impact assessments for data linkages, and greater caution around the use of cross-sector identifiers such as the tax ID.

For more information: DSK Website [DE]

Spain

02/18/2026

Spanish Supervisory Authority | Guidelines | Agentic AI and Data Protection

The Spanish Supervisory Authority (AEPD) has issued guidance on the privacy implications of deploying agentic AI systems.

As a reminder, agentic AI systems operate with a high degree of autonomy and can plan and execute tasks with minimal human intervention. The AEPD identifies several risks arising from this autonomy and complexity, including excessive data collection, uncontrolled memory accumulation, limited auditability, and the possibility of significant actions being taken without adequate human oversight. The guidance highlights key GDPR compliance considerations – such transparency, lawfulness of processing, data minimization and automated decision-making – and recommends measures including memory controls, human supervision and technical safeguards (e.g., strict access management) to mitigate privacy-related risks.

For more information: AEPD Website [ES]

United Kingdom

02/27/2026

ICO | Public Consultation | Research, Archiving and Statistics

The UK Supervisory Authority (ICO) has opened a consultation on updated guidance relating to the research, archiving and statistics provisions under UK data protection law.

Following the introduction of the Data (Use and Access) Act 2025 (DUA Act 2025), the ICO revised its criteria for scientific research and is seeking feedback on the new "disproportionate effort" exemption from the requirement to inform data subjects when previously collected data is re-used for research purposes. The consultation is open until 27 April 2026 and invites stakeholder views on both the substance and impact of the proposed updates.

For more information: ICO Website

02/23/2026

Ofcom | Sanction | Age Assurance Measures

Ofcom has fined an adult-content provider £1.35 million (approx. €1.55 million) for failing to implement age assurance measures.

Under the UK Online Safety Act, providers of adult websites must deploy effective age assurance to prevent children from accessing pornographic material. Shortly after these duties came into force in July 2025, Ofcom launched several investigations into major adult-content websites. Following its investigation, Ofcom concluded that the company had not implemented compliant age assurance measures. It also found that the company had failed to respond to Ofcom's requests in an accurate, complete and timely way, resulting with an additional fine of £50,000 (approx. €58,000).

For more information: Ofcom Website

02/19/2026

Court of Appeal | Judgment | Cyberattacks and Scope of the Security Duty

The Court of Appeal held that organizations must secure personal data they can identify, even if attackers cannot identify individuals from the stolen dataset.

The case arose from an ICO monetary penalty issued after a cyberattack, in which the ICO found that the company failed to implement adequate security measures. The First-tier Tribunal upheld the ICO's findings but reduced the fine from £500,000 to £250,000. On further appeal, the Upper Tribunal concluded that the scraped payment card details were not "personal data" because attackers could not identify individuals from them, meaning the company had no duty to prevent third-party access. The Court of Appeal overturned that approach, confirming that personal data is defined from the controller's perspective, not the attacker's, and that controllers must apply security measures to all personal data they process.

For more information: Court of Appeal's Judgment

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.

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)
Keith Enright – Palo Alto (+1 650.849.5386, kenright@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)