Privacy, Cybersecurity, and Data Innovation Update 12 February 2026

European Data Privacy Newsletter

We are pleased to provide you with the January 2026 edition of Gibson Dunn's monthly European data privacy update. Please feel free to reach out to us to discuss any of these topics further.

Europe

01/27/2026

European Commission | Adequacy Decision | Brazil

The European Commission has adopted an adequacy decision under Article 45 GDPR, allowing EU personal data transfers to Brazil without additional safeguards.

The European Commission found that Brazil's General Personal Data Protection Law provides a level of protection essentially equivalent to the EU data protection framework, permitting personal data to flow from the EU to Brazil without additional transfer mechanisms. On the same day, Brazil adopted its own adequacy decision for personal data transfers from Brazil to the EU.

For more information: European Commission Website

01/23/2026

EDPB | Guidance | EU-U.S. Data Protection Framework

The European Data Protection Board ("EDPB") has updated its Data Protection Framework (DPF) FAQs to provide further guidance for businesses and individuals on EU-US personal data transfers.

The revised FAQs reiterate that exporters should first verify the U.S. recipient's DPF self-certification status and the scope of that certification (including whether it covers any relevant subsidiaries). For transfers of HR data, the FAQs highlight additional steps, such as confirming that the importer's certification includes HR data and informing the importer that the transferred data is HR data. The EDPB also reminds that participation in the DPF does not replace other GDPR obligations.

For more information: Businesses FAQs

01/22/2026

European Commission | Guidance | Data Act

The European Commission has released an updated version of its FAQs on the Data Act.

Developed with input from stakeholders, the FAQs are intended to support the practical implementation of the Data Act. They address topics such as unfair terms in business-to-business data-sharing agreements, switching between data-processing services, and interoperability requirements.

For more information: European Commission Website

01/21/2026

EDPB & EDPS | Joint Opinion | Digital Omnibus on AI

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

In their opinion, the EDPB and EDPS support efforts to reduce the burdens of practical implementation, but caution that administrative simplification must not come at the expense of individuals' rights. They recommend limiting any expanded use of special-category data for bias detection and raise concerns regarding the postponement of provisions relating to high-risk AI systems. The authorities also call for clearer definition of the role of market surveillance authorities, while emphasizing that the independence and powers of data protection authorities should remain preserved.

For more information: EDPS Website

01/20/2026

European Commission | Proposal | New Cybersecurity Package

The European Commission has launched a new cybersecurity package, including a Proposal for a revised Cybersecurity Act.

The revised Cybersecurity Act aims in particular to simplify the European Cybersecurity Certification Framework by introducing streamlined procedures designed to enable the development of certification schemes within 12 months. It would also expand ENISA's powers, strengthening its role in the development of cybersecurity standards. The new cybersecurity package also includes targeted amendments to the NIS 2 Directive intended to enhance legal clarity by simplifying jurisdictional rules, improving the collection of data on ransomware attacks, and facilitating the supervision of cross-border entities through ENISA's reinforced coordinating role.

For more information: European Commission Website

France

01/22/2026

CNIL | Sanction | Data Breach

The French data protection authority (CNIL) fined a French governmental agency €5 million after a cyberattack exposed large-scale jobseeker data, citing major gaps in account security, monitoring, and access controls.

The sanction follows an unauthorized access to personal data relating to individuals registered with the agency over the past 20 years and account users. The CNIL found that security measures were not appropriate under Article 32 GDPR, pointing in particular to overly permissive password settings, lack of MFA for exposed adviser accounts, and insufficient real-time logging/monitoring.

For more information: CNIL Decision [FR]

01/22/2026

CNIL | Sanction | Data Sharing for Advertising Purposes

A company was fined €3.5 million for sharing loyalty-program contact data for ad-targeting without valid consent.

The CNIL sanctioned the company, finding the relied-upon “consent” was not valid because individuals were not properly informed of the targeting purpose. Other infringements identified include insufficient information, security shortcomings, failure to conduct a DPIA, and cookie/trackers compliance issues and was adopted in cooperation with 16 European counterparts given its cross-border impact.

For more information: CNIL Website [FR]

01/16/2026

CNIL | Recommendations | “Multi-device” Consent in Authenticated Environments

The CNIL published recommendations to set out how publishers can lawfully apply a user’s cookie/tracker choices across all devices tied to the same logged-in account without forcing repeated prompts.

The CNIL clarifies that multi-device consent is optional and only relevant in authenticated environments where user choices can be tied to an account and synced across logged-in devices. Consent, refusal, and withdrawal must all carry the same cross-device effect, and users should be informed upfront that their choice applies to all connected devices. The guidance also addresses conflicts between pre-login preferences and account settings, encourages consistent market practices, and highlights privacy-by-design concerns like avoiding the sharing of clear account identifiers with CMP vendors and handling shared devices carefully.

For more information: CNIL Recommendations [FR]

01/14/2026

CNIL | Sanction | Data Breach

The French data protection authority (CNIL) imposed a combined €42 million fine on a French telecom operator following a major customer data breach.

The CNIL reports that attackers accessed personal data tied to around 24 million subscriber contracts. The authority found shortcomings in security (including authentication and monitoring/detection measures), issues in the completeness of information provided to affected individuals, and non-compliant retention practices for certain categories of data. In addition to the fines (€27M for the mobile subsidiary and €15M for the parent company), the CNIL issued

compliance orders with deadlines (notably to complete specific security measures within three months and bring certain retention practices into compliance within six months).

For more information: CNIL Website [EN]

Germany

01/27/2026

Data Authorities | Press Release | Record-High Volume of Data Protection Complaints

German Data Protection Authorities have reported a strong increase in data protection complaints in 2025.

The authority of Lower Saxony received 4,022 complaints in 2025, marking a record high and representing a 70% increase from 2,361 the previous year. Similar trends were reported by various authorities across Germany. This increase reflects greater public awareness and sensitivity to improper data processing, partly driven by the growing digitalization of society.

For more information: LfDI Lower Saxony [DE], LfDI Hamburg [DE] and LfDI Berlin [DE]

01/26/2026

BfDI | Press Release | Privacy Sandbox

Germany's federal DPA has launched "ReguLab," a regulatory sandbox designed to reduce legal uncertainty for privacy-relevant innovation.

This month the BfDI presented ReguLab as a structured environment for organizations to test ideas and discuss data protection requirements early, aiming to accelerate compliant innovation by clarifying how rules apply in practice. The initiative is presented as a joint effort involving the Federal Ministry of the Interior and Community and the federal digital service, with initial focus areas including major public-sector digitization and digital identity building blocks (e.g., eIDAS/EU Digital Identity Wallet).

For more information: BfDI [DE]

12/11/2025

High Court of Frankfurt | Decision | Liability for Third-Party Cookies Extends Beyond Website Operators

The recently published case of the Higher Regional Court (Oberlandesgericht) Frankfurt am Main concerns the liability of third-party service providers for cookie placement without valid user consent under German data-protection and telemedia law.

The court ruled that third-party providers who technically cause or contribute to the placement of cookies without valid user consent can be held liable, even if they are not the primary operator of the website on which the cookies are deployed. This includes third-party analytics, advertising, and tracking providers, even when contracts with website operators stipulate that cookies should only be set with proper consent.

For more information: OLG Frankfurt [DE]

Sweden

01/26/2026

Swedish Supervisory Authority | Sanction | Data Breach

The Swedish Supervisory Authority ("IMY") fined a Swedish digital sports administration platform €560,000 after a data breach.

IMY has fined the platform SEK 6 million (approximately €520,000) for GDPR violations following a January 2025 cyberattack that exposed personal data of over 2.1 million individuals, primarily children and young individuals. The leaked information, which included names, national ID numbers and health data, was subsequently published on the darknet. IMY found that the platform had long been aware of system vulnerabilities but failed to implement adequate technical and organizational safeguards, including real-time intrusion detection, to protect the sensitive data it processed

For more information: IMY Website

Spain

01/19/2026

Spanish Supervisory Authority | Guidance | GenAI use cases

The Spanish Supervisory Authority ("AEPD") released comprehensive GenAI management framework.

In late 2025, the AEPD published its General Policy for the Use of Generative AI, along with a practical annex establishing guidelines for the safe and ethical deployment of AI across the AEPD. In early 2026, it completed its internal framework with key obligations in governance, data protection, transparency, security, and vendor contracting, requiring prior approval of use cases, updated risk inventories, human oversight for automated decisions, and strict data minimization. Organizations are also reminded that GenAI should support, not replace, human decision-making, and must never be relied upon for critical or urgent processes requiring maximum accuracy.

For more information: AEPD Website

01/13/2026

Spanish Supervisory Authority | Informative Note | Risks of using third-party images in AI systems

The Spanish Supervisory Authority ("AEPD") warned of visible and invisible risks in AI image use.

The AEPD published guidance analyzing the risks of using third-party images in AI systems, even in seemingly trivial or playful contexts. The document highlights high-risk scenarios such as sexualization, synthetic intimate content, and the use of images involving minors or vulnerable individuals. It also warns of less visible risks that arise simply from uploading images to AI systems, including loss of control, hidden data retention, and persistent identification risks, even when the output is never published.

For more information: AEPD Website [ES]

United Kingdom

01/21/2026

UK Government I Consultation I Under-16s Social Media Ban

The UK Government has launched a consultation on children's social media use.

The UK Government's consultation examining children's use of mobile phones and social media will consider potential social media bans for children and the role of age assurance technologies. The consultation is expected to last three months with the UK Government's response anticipated in the summer.

Alongside this consultation, an amendment was introduced during the passage of the Children's Wellbeing and Schools Bill that would require the introduction of regulation raising the minimum age for social media access to 16. The Bill will move to the House of Commons, where ministers have signalled in the press they would seek to overturn the amendment and instead await the outcome of the consultation.

For more information: Consultation, Amendment, House of Lord website and Press Reporting

01/19/2026

UK Government I Memorandum of Understanding I Data protection

UK Department for Science, Innovation and Technology has published a Memorandum of Understanding (MOU) between the Information Commissioner's Office (ICO) and the UK Government.

This MOU formalises the ICO and UK Government's framework for cooperation on data protection. The MOU commits ministers and senior officials to earlier engagement with the regulator, regular assurance exercises and the creation of a data safety culture.

For more information: UK Government Website

01/15/2026

ICO I Guidance I International Transfers

The ICO has published updated guidance on international transfers.

This updated guidance does materially alter the substance of the ICO's historic advice on international transfers but is intended to simplify the guidance for businesses. The updated guidance sets out a 'three step test' for organisations to use to help identify if they are making

restricted transfers and reiterates the mechanisms available to ensure an equivalent level of protection for transferred data.

For more information: ICO

01/08/2026

ICO I Guidance I Agentic AI

The UK Information Commissioner's Office (ICO) has published a report on the rise of agentic AI.

The ICO's new report on agentic AI identifies certain key data protection compliance concerns, including in relation to transparency, purpose limitations in circumstances where the purpose of the agentic AI is unclear, data minimisation, and concerns in relation to automated decision-making (ADM). The report also notes that "[t]hroughout 2026 the ICO will actively monitor advancements and work with AI developers and deployers to ensure they are clear on what the law requires of them", with a statutory code on AI and ADM being developed by the ICO and further regulatory guidance on agentic AI, ADM and profiling expected Q1 2026.

For more information: ICO report

01/07/2026

ICO I Investigation I AI Provider

The UK Information Commissioner's Office (ICO) published a public statement in response to a social media and AI provider.

Following a statement on 7 January that the ICO had contacted a social media and AI provider to seek "clarity on the measures they have in place to comply with UK data protection law and protect individuals' rights", the ICO announced on 3 February it had opened formal investigations into the provider over the AI's processing of personal data and the AI's alleged generation of harmful sexualised content. The ICO's investigation will also look into whether "appropriate safeguards were built into [the AI's] design and deployment." Alongside the data protection authority's investigation, Ofcom and the European Commission have also launched investigations on 12 January into this social media and AI provider over the AI's sexualised imagery under the Online Safety Act and the Digital Services Act respectively.

For more information: ICO Statement, ICO Investigation Announcement

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)
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)