Privacy, Cybersecurity, and Data Innovation Update 14 January 2026

European Data Privacy Newsletter

December 2025

Europe

12/22/2025

European Commission | Data Transfers | EU-UK Adequacy Decisions

The European Commission has renewed the adequacy decisions with the United Kingdom under both the GDPR and the Law Enforcement Directive.

This renewal follows a temporary extension granted in June 2025, which enabled the Commission to conduct a comprehensive assessment of the UK's legal framework in light of recent amendments introduced by the Data (Use and Access) Act. The Commission concluded that the UK's data protection regime continues to provide a level of protection that is essentially equivalent to that of the European Union. The new decisions are subject to a sunset clause of six years, running until 27 December 2031, with the possibility to be renewed.

For more information: European Commission Website

12/16/2025

European Commission | Data Act | Legal Helpdesk

The European Commission has launched a legal helpdesk to support the practical application of the Data Act.

The helpdesk is intended to provide guidance on compliance with the Data Act's requirements by enabling stakeholders to submit questions directly. It complements existing support tools including FAQs and Draft Recommendation on non-binding Model Contractual Terms for data access and use (MCTs) and non-binding Standard Contractual Clauses for cloud computing contracts (SCCs).

For more information: European Commission Website

12/12/2025

European Union | Regulation | Procedural Rules on the Enforcement of the GDPR

Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679 ("GDPR") has been published.

The new regulation aims to improve cooperation between supervisory authorities, accelerate the complaint handling process, and make the GDPR enforcement more efficient in cross-border cases. It will enter into force 20 days after publication and will apply 15 months thereafter.
For more information: Official Journal of the European Union

12/09/2025

Confederation of European Data Protection Organizations | Data Act | FAQ

The Confederation of European Data Protection Organizations ("CEDPO") has published FAQs on the Data Act's access-by-design and data-sharing requirements.

The FAQs are intended to support Data Protection Officers by clarifying the scope, key concepts, and core obligations of the Data Act. They also address issues at the intersection of the Data Act and the GDPR, including the impact of the Data Act on the handling of data subjects' rights and

the legal bases available for the processing of personal data to which the Data Act applies.
For more information: CEDPO Website

12/03/2025

European Data Protection Board | Recommendations | Creation of User Accounts on E-commerce Websites

The European Data Protection Board ("EDPB") has adopted recommendations on the legal basis for requiring the creation of user accounts on e-commerce websites.

Although e-commerce controllers may have a business interest in requiring users to create an account, the EDPB emphasizes that doing so can expose individuals to additional risks concerning their rights and freedoms. Therefore, these recommendations provide guidance to e-commerce controllers on the circumstances under which they may lawfully require users to create an account. The recommendations are subject to public consultation open until February 12, 2026.

For more information: EDPB Website

12/02/2025

Court of Justice of the European Union | Judgment | Hosting Providers' Status and Liability

The Court of Justice of the European Union ("CJEU") issued a landmark ruling on the scope of liability for hosting providers under EU law.

The Court held that hosting providers may be considered joint controllers together with the advertisers for personal data in advertisements if they exert a decisive influence over the processing for their own purposes thereby going beyond a neutral intermediary role. The Court clarified that operators cannot rely on the liability exemptions for neutral intermediaries (under the E-Commerce Directive) to avoid GDPR obligations. This decision sets an important precedent for interpreting the concept of "controller" under the GDPR in the context of online platforms and reinforces the need for providers to implement robust compliance mechanisms – such as verifying advertisers' identities for ads containing sensitive data – to avoid assuming legal responsibility for third-party content.

For more information: CJEU Website

France

12/22/2025

French Supervisory Authority | Sanction | Data Breach

The French Supervisory Authority ("CNIL") imposed a €1,700,000 fine on a French IT company following a data breach, for failing to implement sufficient security measures.

The company, which specializes in the design of IT systems and software, was investigated after customers reported personal data breaches in 2022. The CNIL found that security vulnerabilities in the company's software resulted from a failure to apply basic and state-of-the-art security measures, despite the company being aware of these issues through prior audit reports. These failings were considered aggravated given the company's core IT-related activities.

For more information: CNIL Website

12/12/2025

French Supervisory Authority | Experimental Tool | AI Traceability

The French Supervisory Authority ("CNIL") has launched an experimental tool to explore the traceability of AI models published in open source.

The tool maps genealogical links between open-source AI models, enabling the identification of models within the same family tree that may have stored personal data relating to the same data subject. The project aims to contribute to the CNIL's analysis of practical scenarios for exercising data subject rights, such as access, erasure, and objection.

For more information: CNIL Website [FR]

12/11/2025

French Supervisory Authority | Sanction | Data Breach

The French Supervisory Authority ("CNIL") imposed a €1,000,000 fine on a data processor following a data breach affecting a controller.

In November 2022, a music streaming platform notified the CNIL of a data breach involving the publication of user data on the darknet and implicating its processor. Following investigations conducted in 2023 and 2024, the CNIL found that the processor had failed to comply with several GDPR obligations. In particular, it retained personal data relating to more than 46 million users after termination of the contract with the controller, processed the data without instructions to enhance its own services, and failed to maintain a record of processing activities in its capacity as a processor.

For more information: CNIL Website [FR]

Germany

12/12/2025

German Supervisory Authority | Guidance | Data Protection Certification Programs

The Data Protection Conference ("DSK") has updated its guidelines on the requirements for data protection certification programs under the GDPR.

The DSK has issued guidelines setting out minimum requirements for GDPR certification programs under Article 42 of the GDPR. The guidelines outline certification criteria, audit methods, and assessment standards aligned with ISO IEC 17067, covering lawful processing, data protection by design, security, and data subject rights.

For more information: DSK Website [DE]

12/12/2025

German Supervisory Authority | Statement | Proposition of a GDPR Reform

The Data Protection Conference ("DSK") has issued a statement criticizing the European Commission's proposed GDPR reform for failing to deliver meaningful relief for small and medium-sized enterprises (SMEs).

According to the DSK, the draft neglects legislative adjustments that could reduce compliance burdens for SMEs, thereby missing the Commission's own objective of cutting bureaucracy. The DSK emphasizes that effective reform should balance administrative simplification with robust data protection standards, warning that the current proposal risks undermining both goals. Instead, the DSK proposes a shift toward "manufacturer liability," arguing that IT providers should be legally required to design compliant products. This would lift the primary compliance burden from SMEs, who often lack the leverage to enforce data protection standards in the software they utilize.

For more information: DSK Website [DE]

12/06/2025

German Parliament | Legislation | NIS-2 Implementation Act

On 6 December 2025, the German NIS-2 Implementation Act came into effect, transposing the EU NIS-2 Directive into national law and imposing stricter cybersecurity obligations on operators of essential and important entities.

The law requires organizations to promptly assess whether they fall within its scope, implement risk management measures, and prepare for enhanced reporting duties regarding security incidents. Companies must also ensure compliance with governance requirements, including management accountability and documentation of security processes. Failure to comply may result in significant administrative fines, making immediate action critical for affected entities.

For more information: Bundesgesetzblatt [DE]

12/05/2025

Supervisory Authority North-Rhine Westphalia | Fine | Transparency and Accountability

The Supervisory Authority of North-Rhine Westphalia ("LDI NRW") has imposed a fine of €300,000 on a telecommunications company for persistent violations of transparency and accountability obligations under the GDPR.

According to the authority, the company repeatedly failed to comply with access requests from data subjects and demonstrated a lack of cooperation during complaint proceedings. These practices were deemed to infringe the core principles of lawful processing, transparency and the right to erasure. The enforcement action highlights the regulator's strict stance on compliance

within the telecommunications sector, especially when systemic deficiencies in data handling and responsiveness to data subject rights are identified.

For more information: LDI NRW [DE]

12/04/2025

German Federal Government & Länder | State Modernization | Federal Modernization Agenda

The German Federal Government and the Länder have adopted the Federal Modernization Agenda, a joint reform initiative aimed at reducing bureaucracy, accelerating administrative procedures, and advancing the digital transformation of public services.

The agenda includes measures to streamline administrative processes, particularly in the context of infrastructure projects. It also foresees a review of regulatory obligations, including in the area of data protection, with the aim of reducing administrative burdens while maintaining an adequate level of protection. The initiative serves as a strategic framework for improving efficiency and responsiveness within Germany's federal system.

For more information: BMDS [DE]

Italy

11/27/2025

Italian Supervisory Authority | Sanction | Marketing Practices

The Italian Supervisory Authority ("Garante") fined a security company €400,000 for unlawful direct marketing practices.

The Garante found that the company continued sending promotional messages despite objections, bundled marketing consent with quote requests, and retained prospect data for an excessive 12 months. In addition to the fine, the Garante ordered the company to cease unlawful processing, delete data collected without valid consent, update its disclosures to meet the GDPR

requirements, and report compliance actions within 60 days, noting remedial steps were already underway.

For more information: Garante Website [IT]

11/27/2025

Italian Supervisory Authority | Sanction | Security | Marketing Practices

The Italian Supervisory Authority ("Garante") fined a distributor of water and natural gas €300,000 for processing customer data without adequate security measures and valid legal basis for marketing purposes.

The investigation launched by the Garante found that anyone could register in a customer's name using only a tax code and any email, gaining access to personal data. Consent boxes for privacy, advertising, and customer satisfaction were pre-checked, violating EU rules and transparency requirements. The processing also breached data retention limits.

For more information: Garante Website [IT]

United Kingdom

12/18/2025

UK Supervisory Authority & Crown Dependencies | Investigation | Cross-Border Breach

The UK Supervisory Authority ("ICO") launched a joint investigation with Jersey, Guernsey, and Isle of Man authorities into a cyber incident affecting a trade union.

The ICO announced a coordinated enforcement action alongside data protection authorities from the three Crown Dependencies regarding a significant data breach affecting a trade union representing technology and science professionals. The breach reportedly exposed sensitive data (e.g., trade union membership, religious belief) of union members across these jurisdictions. The regulators highlighted that this joint approach reflects a new operational model for tackling complex cross-border incidents where data subjects in the UK and its dependencies are affected

by the same cyber event.
For more information: ICO Website

12/05/2025

UK Supervisory Authority I Regulatory Action I Cookie Compliance

The UK Supervisory Authority ("ICO") published an update on its cookie compliance review.
In January 2025, the ICO had announced a review of cookie compliance across the UK's top 1,000 websites. On 4 December 2025, the ICO published an update on their review, noting that over 95% (979) of the UK's top 1,000 websites now meet its compliance checks, with many organizations improving their practices after direct regulatory engagement (including warning letters and preliminary enforcement notices). Interim Executive Director of Regulatory Supervision, Tim Capel, said "we will continue to monitor compliance and engage with industry to ensure they uphold their legal obligations, while also supporting innovation that respects people's privacy." The next update on this work will be provided in 2026.
For more information: ICO 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)
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)