View in browser

Privacy, Cybersecurity, and Data Innovation Update September 9, 2026

European Data Privacy Newsletter

We are pleased to provide you with the July-August 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.

European Union

07/27/2026

European Commission | Guidance | Cyber Resilience Act

The European Commission has published its guidance on the application of the Cyber Resilience Act (CRA), the EU regulation setting mandatory cybersecurity requirements for hardware and software products with digital elements throughout their lifecycle.

The non-binding guidance clarifies how key provisions should be interpreted and applied. It focuses on remote data processing solutions, free and open-source software, the notion of "support periods", and the interplay between the CRA and other EU legislation. The guidance elaborates on core obligations such as risk assessments, reporting duties and vulnerability handling. The Cyber Resilience Act's main obligations apply from 11 December 2027, with reporting obligations applying as of 11 September 2026.

For more information: European Commission Website / European Commission Guidance

07/23/2026

European Commission | Report | Adequacy Decision for the Republic of Korea

The European Commission finds that the Republic of Korea continues to provide an adequate level of protection of personal data.

The 2021 adequacy decision for the Republic of Korea allows the free flow of personal data from the European Union to this country. In its first review of this adequacy decision, the Commission confirms that the Republic of Korea continues to provide an adequate level of protection for personal data transferred. The report includes recommendations to further reinforce some of the safeguards provided by the South Korean framework, while acknowledging that the EU and Korean data protection frameworks have converged further.

For more information: European Commission Website

07/14/2026

EDPB | Decision | Objection to the Lead Supervisory Authority (LSA)

EDPB requires Belgian DPA to handle the merits of NOYB cookie banner complaint.

The decision concerns a dispute submitted by the Belgian Data Protection Authority (DPA) about a complaint against a Belgium-based company. The Belgian DPA, acting as Lead Supervisory Authority (LSA), proposed to dismiss the complaint on the basis of an abuse of Art. 77 GDPR and Art. 80(1) GDPR. The Austrian DPA, acting as a Concerned Supervisory Authority (CSA) since the complaint was lodged by the Austrian-based NGO Noyb, objected but the Belgian DPA still submitted the case to the EDPB. The EDPB considered the Austrian DPA's objection relevant and instructed the Belgian DPA to not dismiss the complaint and to assess it on its merits. The LSA should now submit a new draft decision to the CSAs.

For more information: EDPB Website / EDPB Binding Decision 1/2026

07/08/2026

EDPB | Guidelines | Anonymization, Web Scraping and Blockchain

The EDPB has adopted guidelines on anonymization, on web scraping in the context of generative AI and the final version of its guidelines on the processing of personal data through blockchain technologies.

The new guidelines on anonymization bring clarity to the notion of anonymous data but also provide a practical framework for organizations to determine if anonymization is successful. In its guidelines on web scraping in the context of generative AI, the Board clarifies aspects of GDPR compliance of web scraping including the legal basis for such activities. These guidelines will be subject to public consultation until 30 October 2026. The EDPB also adopted the final version of its guidelines on blockchain technologies that can help organizations using blockchain technologies to comply with the GDPR.

For more information: EDPB Website / Guidelines 02/2026 on Anonymisation, Guidelines 03/2026 on web scraping in the context of generative AI and Guidelines 02/2025 on processing of personal data through blockchain technologies

France

08/10/2026

CNIL | Note | Data Protection Officer and Conflicts of Interest

The CNIL has published a note on how to identify and manage conflicts of interest arising from the DPO function.

DPOs will be in a situation of conflict of interest if they are entrusted with both the missions of Article 39 of the GDPR and missions likely to harm their performance, in particular where the additional tasks undermine the DPO's independence. The CNIL recommends carrying out an analysis of potential conflicts of interest before assigning any new functions or tasks to the DPO.

For more information: CNIL Website [FR]

07/22/2026

CNIL | Tool | Pixels Recommendation

The CNIL published a Q&A answering the main questions raised by professionals regarding the implementation of its recommendation on pixels.

The professionals concerned have been required to comply with the CNIL's recommendation on tracking pixels since 14 July 2026. The Q&A covers the scope of the recommendation, the responsibility of operators, the question of exempted pixels, the practical arrangements for obtaining consent, as well as the arrangements for applying the recommendation over time.

For more information: CNIL Website [FR]

07/09/2026

CNIL | Advice | Monitoring of Employed Person's Activity

An employer has the power to oversee and monitor the activity of its staff and their use of workplace equipment. Nevertheless, this power cannot be exercised in an excessive manner and, depending on the technologies used, specific rules may apply.

As a general rule, the CNIL considers that three cumulative conditions apply to the employer before it can install a system for monitoring workers' activity. To be lawful, a system for monitoring staff activity must cumulatively satisfy the tests of justification and proportionality, be submitted to the employee representative bodies and be brought to the attention of the employees.

For more information: CNIL Website [FR]

07/07/2026

CNIL | Advice | Mobile Apps and Geolocation

Following the publication of its recommendation on mobile applications, the CNIL has issued a reminder of the rules applicable to the collection and use of geolocation data from mobile apps.

Given the sensitivity of geolocation data and the risks associated with its use, the CNIL reminds that stakeholders must ensure compliance with applicable data protection rules. In this context, the CNIL is recalling the rules applicable to this personal data, as well as individuals' rights to protect their privacy.

For more information: CNIL Website [FR]

07/02/2026

CNIL | Guide | Processing Of Players' Data By Gambling Operators

To support operators, the French gambling regulator (ANJ), working closely with the CNIL, has published a non-binding guide clarifying how data protection rules apply in this sector.

Gambling operators process large volumes of personal data on players every day such as identity, contact details, banking data, financial transactions and gaming activity. This processing must comply with the GDPR while also meeting sector-specific obligations, particularly around preventing excessive gambling and combating money laundering and terrorist financing. The guide only covers processing tied to gambling activities under ANJ's jurisdiction.

For more information: CNIL Website and the CNIL and ANJ Guide on the processing of players' data by gambling operators [FR]

Germany

08/13/2026

BfDI | Press Release | Cookie Banners and Consent Management Services

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) published recommendations on the handling of cookie banners and called for binding, machine-readable privacy preferences and consent management services to be anchored in EU law in further proceedings on the Digital Omnibus.

The recommendations are based on a nationwide survey according to which 60% reject cookies where this is possible with a single click, and 83% consider it important that their settings apply across all websites. The BfDI recalls that the Commission's original Digital Omnibus proposal contained a provision (Article 88b GDPR) on automated, machine-readable consent and objection signals which was dropped by the Council and urges the co-legislators to revisit the issue in further negotiations.

For more information: BfDI Website [DE]

07/02/2026

Federal Government | Reform Program | Simplification of Data Protection Law

The coalition committee of CDU/CSU and SPD agreed on a reform program that includes plans to simplify German data protection law and to concentrate supervisory competences at the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

The Federal Government intends to simplify national data protection law and make consistent use of the opening clauses of the GDPR and will advocate at EU level for non-commercial activities (such as those of associations), small and medium-sized enterprises and low-risk processing operations to be excluded from the scope of the GDPR. A national Data Code is to harmonize and simplify data law, procedures are to be streamlined and supervisory structures simplified and bundled, including a concentration of competences at the BfDI. The independent data protection authorities of the Länder favor coordination within the existing federal structure over centralization; they support a Bundesrat bill, introduced on 10 July 2026, that would give the Data Protection Conference (DSK) a statutory basis while retaining supervision at Länder level.

For more information: Federal Government and LfDI Baden-Württemberg and Bundesrat [DE]

Netherlands

08/27/2026

Autoriteit Persoonsgegevens | Announcement | Mandatory Publication of GDPR Sanctions

As of 1 September 2026, the Dutch DPA (AP) is legally required to publish the administrative sanctions it imposes for violations of the GDPR.

Following an amendment to the Dutch GDPR Implementation Act (UAVG), the publication of administrative sanctions imposed by the Dutch DPA (AP), such as fines, orders subject to penalty payments and processing bans, becomes a legal obligation rather than a matter of the authority's own publication policy. The AP, which has long requested this legislative change, considers that the publication of sanctions strengthens legal certainty, makes enforcement more effective and enables other organizations to learn from identified infringements. The AP will also

publish sanctions imposed under the Dutch Police Data Act and the Judicial and Criminal Records Data Act in the same manner.

For more information: AP Website [NL]

07/13/2026

Autoriteit Persoonsgegevens | Guide | New GDPR Guidelines for Generative AI

The Dutch Data Protection Authority (DPA) publishes two new documents that help organizations with the responsible development and deployment of generative AI under the GDPR.

The DPA sets out that, while generative AI offers social and economic opportunities, there are also risks to fundamental rights such as the protection of personal data. The GDPR guide for developers of generative AI models outlines how generative AI can be used safely, responsibly and in line with fundamental rights. While this guidance provides legal frameworks for developers, the practical tool gives substance to the guide by supporting organizations looking to acquire, deploy, and use generative AI. This tool helps controllers determine which GDPR obligations apply and which technical and organizational measures are needed.

For more information: Autoriteit Persoonsgegevens Website, the Guidance and the Practical tool [NL]

Denmark

07/01/2026

Datatilsynet | Statement | U.S. Supreme Court's Ruling May Affect The DPF

Datatilsynet (Danish DPA) is monitoring developments following the U.S. Supreme Court's ruling in *Trump v. Slaughter* and is urging data controllers to revisit their assessments regarding transfers of personal data to the United States.

The DPA is monitoring the case and, through the European Data Protection Board (EDPB), is assessing what effects the ruling may have on the validity of the adequacy decision underpinning the EU-US Data Privacy Framework (DPF). The DPF remains valid for now until the European Commission or the Court of Justice of the EU declares it invalid. The ruling could also affect transfers made on other legal

bases and the DPA is calling on data controllers to revisit the country assessment within their Transfer Impact Assessments (TIAs).

For more information: Datatilsynet Website [DK]

Spain

07/21/2026

AEPD | Report | Processing of Personal Data with AI

The Spanish DPA (AEPD) published a report on the accuracy, suitability and quality of data in processing personal data with Artificial Intelligence.

The report examines the relationship between data quality and the GDPR's principle of accuracy in the processing of personal data, arguing that both must be interpreted in light of the purpose pursued and the suitability of the processing. While the two concepts are related, they are not equivalent. Data quality is the broader of the two, covering both personal and non-personal data, whereas the accuracy principle should not be limited to the veracity or currentness of data. This distinction matters particularly in the context of AI, where governance processes must align data protection obligations with the demands of developing and deploying AI systems throughout their life cycle.

For more information: AEPD Report [EN]

United Kingdom

08/26/2026

ICO | Progress Update | Children's Code Strategy

The ICO published a progress update on its Children's Code strategy.

The ICO's Children's Code strategy, launched in April 2024, focuses on social media platforms (SMPs) and video sharing platforms (VSPs). Since its previous update of December 2025, the ICO notes that it has launched risk reviews of 14 age assurance providers (with targeted recommendations and monitoring to follow), taken enforcement action in relation to alleged unlawful use of children's personal information, and secured commitments from some SMPs to strengthen their age

assurance measures and improve transparency. Addressing the government's recently announced proposal to prohibit certain platforms from offering their services to children under 16 through amendments to the Online Safety Act, the ICO emphasized that data protection obligations apply irrespective of any minimum age or service restriction. The Children's Code will therefore continue to apply to the services concerned, as well as to other SMPs, VSPs and gaming platforms likely to be accessed by children. The ICO indicated that it will continue to engage with the government and other regulators, in particular Ofcom, on the implementation of the proposals.

For more information: ICO Website

07/15/2026

UK Government | Announcement | Information Commission Board

Seven non-executive members appointed to Information Commission Board, supporting the move to a new board-led governance model.

The Information Commission Board will take over all the functions and responsibilities of the Information Commissioner's Office (ICO). It was established by the Data (Use and Access) Act 2025 to succeed the ICO as the United Kingdom's independent data protection authority. The appointment of the new non-executive members forms an important part of the transition to this new governance model and will help shape the Information Commission's strategic direction.

For more information: UK Government Website

The following Gibson Dunn lawyers prepared this update: Ahmed Baladi, Vera Lukic, Kai Gesing, Joel Harrison, Thomas Baculard, Ioana Burtea, Kelly Cannon, 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)