View in browser

Privacy, Cybersecurity, and Data Innovation Update

July 9, 2026

European Data Privacy Newsletter

We are pleased to provide you with the June 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

06/26/2026

EDPB | One-Stop-Shop Case Digest | Data Subject Rights

The European Data Protection Board (EDPB) published an updated One-Stop-Shop (OSS) case digest on the right to object and the right to erasure.

The case digest is based on the key One-Stop-Shop (OSS) decisions and provides insights into how EU supervisory authorities assess organizations' internal procedures for handling data subject requests. The updated version incorporates hundreds of new OSS decisions adopted since the publication of the original digest, including cases concerning objections to direct marketing and requests for the deletion of user accounts or online profiles. It identifies recurrent infringements and summarizes corrective measures imposed by EU supervisory authorities.

For more information: EDPB Website

06/24/2026

EDPB | Contact Form | GDPR Enforcement

The European Data Protection Board (EDPB) launched a dedicated contact form for stakeholders to report possible inconsistencies in GDPR interpretation across Europe.

The form allows stakeholders to flag alleged divergences between national positions, or between national positions and EDPB guidance. The initiative follows the EDPB's Helsinki Statement on enhanced clarity, support and engagement, and is intended to support more consistent GDPR enforcement across Europe. The EDPB will not respond to individual submissions but plans to regularly compile and discuss the information at Board level to consider possible consistency measures.

For more information: EDPB Website

06/18/2026

CJEU | Judgment | Parallel Exercise of GDPR Complaint and Judicial Remedies

The Court of Justice of the European Union (CJEU) ruled that a supervisory authority cannot reject a GDPR complaint solely because court proceedings on the same subject matter are already pending.

The CJEU held that Article 77(1) and Article 79(1) GDPR must be interpreted as precluding a supervisory authority, with which a complaint has been lodged under Article 77(1), from rejecting that complaint on the sole ground that judicial proceedings under Article 79(1) concerning the same subject matter have already been brought, even where the decision given in those proceedings is not yet final. The ruling confirms that the administrative remedy before a supervisory authority and the judicial remedy against a controller or processor may be exercised in parallel and independently of each other.

For more information: CJEU Website

06/10/2026

EDPB | Public Consultation | Data Breach Notification Template

The European Data Protection Board (EDPB) has adopted a draft template for personal data breach notifications, which is now subject to public consultation.

The template is intended to harmonize data breach notification processes across supervisory authorities and assist organizations in ensuring that notifications contain all information required under Article 33 GDPR. Following the consultation period, which runs until 5 August 2026, the EDPB will determine the timeline for implementation by supervisory authorities.

For more information: EDPB Website

06/03/2026

European Supervisory Authorities | Report | Major ICT-Related Incidents under DORA

The European Supervisory Authorities (ESA) published their first annual overview of major ICT-related incidents under the Digital Operational Resilience Act (DORA).

As a reminder, the ESAs comprise the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA). The report analyzes 3,383 major ICT-related incidents reported by financial entities, with around one third involving a cross-border impact. The ESAs found that system failures and external events were the main drivers, while only 10% of reported incidents related to cybersecurity. The authorities called attention to third-party risk management, oversight of outsourced services, coordination with providers during incident response and recovery, and resilience against risks linked to advanced AI-driven tools.

For more information: ESMA Website

Belgium

05/29/2026

Belgian Supervisory Authority (APD) | Investigation Findings | AI Chatbots, Innovation and Data Protection

The APD published findings from an Inspection Service investigation into an AI conversational smartphone application.

The APD found that developers and operators of AI chatbots prioritized product development, user experience, and scalability over GDPR and privacy compliance. It identified concerns around free-text interactions containing sensitive personal data, data minimization, purpose limitation, storage periods, transparency on internal processing, model retraining and sharing with external providers. The authority recommended clearly allocating roles within complex AI ecosystems, conducting DPIAs before deployment and integrating data protection requirements from the design phase.

For more information: APD Website [FR]

France

06/30/2026

French Supervisory Authority (CNIL) | Recommendation | Location Data from Connected Vehicles

The CNIL has published a Recommendation on the use of location data from connected vehicles by professionals to provide greater transparency for users.

The Recommendation's objective is to provide a clear and up-to-date framework to support stakeholders in the connected-vehicle ecosystem, including manufacturers, fleet managers, telematics providers and data aggregators. It recalls the legal requirements governing the collection and use of personal data and provides practical guidance on transparency, data minimization, retention, security and the exercise of users' rights. In particular, the Recommendation helps stakeholders identify the purposes for which user consent is required, or may be exempted, under Article 82 of the French Data Protection Act (*Loi Informatique et Libertés*). The Recommendation also addresses the management of individuals' rights where

different individuals may use the same vehicle, including through authenticated user profiles.

For more information: CNIL Website and Recommendation [FR]

06/19/2026

CNIL | Guidance | Data Security

The CNIL published updated guidance on essential security measures to help organizations protect personal data and business activity.

The guidance lists baseline measures, including strong passwords, password managers, multi-factor authentication, phishing vigilance, official software sources, automatic updates, regular offline backups, antivirus and firewall tools, device encryption, separation of personal and professional uses, travel precautions and staff training. It also links data security to GDPR minimization and retention principles and recalls breach response steps, including notifying the CNIL where personal data is affected.

For more information: CNIL Website [FR]

06/10/2026

CNIL | Guidance | Commercial Prospecting Rules

The CNIL has published guidance on consent, information and opt-out requirements for commercial prospecting.

The guidance recalls that commercial prospecting by email, SMS/MMS and automated calls generally requires prior consent for individuals, subject to limited exceptions. By contrast, B2B prospecting may rely on legitimate interest where the solicitation relates to the recipient's professional activity and the recipient is given a simple and free opt-out. The CNIL also explains that, from 11 August 2026, commercial telephone prospecting to consumers will require prior consent unless the call concerns an ongoing contract, with further implementing texts expected.

For more information: CNIL Website [FR]

06/10/2026

CNIL | Guidance | Transfer of Consumer Data to Partners for Prospecting

The CNIL has published guidance on the conditions under which consumers' contact data may be transferred to partners for commercial prospecting purposes.

The CNIL states that organizations transferring customer or prospect data to partners must comply with GDPR obligations, including data minimization, retention, security, facilitation of rights and proof of valid consent where required. For partner prospecting by email, SMS, automated call or telephone where consent is required, the organization transferring the data must obtain prior consent and inform individuals of partner identities and purposes, including through an exhaustive and updated partner list.

For more information: CNIL Website [FR]

Germany

06/24/2026

German Parliament | Legislation | IP Address Retention

The German Bundestag held the first reading of the Federal Government's bill introducing a three-month retention obligation for IP addresses.

The bill would require internet access providers to retain the IP addresses assigned to their customers, together with the associated port numbers, for three months. The aim is to enable law enforcement and other authorized authorities to reliably identify the holder of an internet connection. Following the debate on 24 June 2026, the bill was referred to the parliamentary committees, with the Committee on Legal Affairs and Consumer Protection taking the lead in further discussions.

For more information: German Parliament [DE]

06/22/2026

Federal Office for Information Security (BSI) | IT Security Information Note | AI-Driven Cyber Risks

The BSI published an IT security information note on the impact of AI developments on organizational cybersecurity.

The BSI warned that AI developments are changing the cyber threat landscape and reducing the time available for defensive response, including by accelerating vulnerability discovery, analysis and exploitation. The note recommends reducing attack surfaces, improving patch management, strengthening detection and incident response, applying standard controls such as least privilege, multi-factor authentication and backups, and adopting an “assume breach” posture for exposed systems and newly patched weaknesses.

For more information: BSI press release and Note [DE]

06/18/2026

German Data Protection Conference (DSK) | Position Paper | Modernization of Data Protection Supervision and Data Protection Law

The independent data protection authorities of the German Länder have adopted the "Stuttgart Impulses for the Modernization of Data Protection" and opened them for consultation.

The position paper, adopted in the context of the 111th Data Protection Conference (DSK), sets out ten proposals to modernize data protection supervision while retaining supervision within Germany’s federal structure. Key proposals include creating a statutory basis for the DSK in the Federal Data Protection Act (BDSG), binding majority decisions of the DSK for the non-public sector, establishing a single point of contact for companies and research institutions operating in several Länder, and recognizing decisions taken by one supervisory authority in matters spanning several Länder. The paper also contains core positions on substantive data protection law, including strengthening the protection of children online and facilitating research in the public interest.

For more information: LfDI Baden-Württemberg [DE]

06/09/2026

Regional Court Berlin | Judgment | Reduction of GDPR Fine in Tenant Data Case

The Regional Court of Berlin upheld the GDPR liability of a listed German real estate company for failing to delete former tenants' data, while reducing the fine imposed by the Berlin DPA.

The proceedings arose from a 2019 fining decision by the Berlin Commissioner for Data Protection and Freedom of Information, which found that the company had used an archive system that did not allow personal data of former tenants to be deleted once no longer required. The court found infringements of the principles of data minimization and storage limitation, but reduced the fine from EUR 14,5 million to EUR 900,000, taking into account, in particular, that the violations occurred during the GDPR's introduction phase and that the company had cooperated with the authority.

For more information: Regional Court Berlin [DE]

Norway

06/03/2026

Datatilsynet | GDPR Complaint | "Consent or Pay" Model

Datatilsynet confirmed that the Norwegian Consumer Council and a privacy advocacy organization had filed a complaint against a major Norwegian media group over its "consent or pay" model.

The complaint relates to the group's implementation of the model across several of its news outlets, where readers must either consent to tracking and behavioural advertising or pay a monthly fee for an ad-free, privacy-respecting alternative. The complainants argue that consent to tracking cannot be regarded as freely given and therefore valid under the GDPR when the alternative is payment. Datatilsynet confirmed receipt of the complaint, noted that it had also received several other complaints and more than 100 tips concerning the model, and stated that it will assess the legality of the arrangement as part of its ongoing review.

For more information: NCC press release and Complaint

06/01/2026

Datatilsynet | Enforcement | Fine for Invalid Customer Club Consent

Datatilsynet fined a major Nordic consumer electronics retailer NOK 20 million (€1,832,094) for processing personal data in its customer club without valid consent.

The authority found several GDPR infringements following a June 2022 audit of the retailer's Nordic and Norwegian entities, including failure to obtain valid consent, failure to assess new processing purposes, insufficient assessment of legitimate interests and failure to respond to data subject rights requests within the GDPR deadline. Datatilsynet found that more than six million customer club members in the Nordic region were affected.

For more information: Datatilsynet Website and Decision [NO]

Portugal

06/22/2026

National Cybersecurity Centre | Regulation | NIS2 Implementation

The Portuguese CNCS published Regulation No. 756/2026 implementing the national Cybersecurity Legal Framework established by the Decree-Law No. 125/2025 transposing the NIS 2 Directive.

The regulation implements Decree-Law No. 125/2025, and applies to essential entities, important entities and relevant public entities within the regime. It defines rules for the electronic platform used for identification, qualification, communications and notifications with cybersecurity authorities, and addresses compliance levels, risk-management duties, incident notification and governance contacts.

For more information: Regulation No. 756/2026 [PT]

Spain

06/18/2026

AEPD and Belgian APD | Recommendations | Data Protection in Video Games

The Spanish (AEPD) and Belgian (APD) supervisory authorities published Joint Recommendations on GDPR compliance in the video game sector.

The Recommendations set out GDPR best practices for organisations involved in the development, publishing, distribution, and operation of video games. It examines how personal data is processed throughout the gaming lifecycle (including account creation, telemetry, behavioural analytics, profiling, and automated decision-making) identifies associated privacy risks, and provides lifecycle-based recommendations and role-specific checklists to help industry participants embed data protection by design and maintain GDPR compliance.

For more information: AEPD Website [ES]

United Kingdom

06/23/2026

ICO | Enforcement | Unlawful Marketing Texts

The ICO fined a debt-solutions marketing firm £300,000 (€348,236) for sending more than 5.5 million unlawful direct marketing texts.

The ICO found that over three years the firm sent 5,575,715 unsolicited direct marketing texts promoting debt solutions to people who had been refused loans, generating more than 60,000 complaints to the ICO and the 7726 spam-reporting service. The messages included fabricated bailiff threats designed to pressure recipients, and the ICO found breaches of Regulations 22 and 23 PECR and issued an enforcement notice requiring the firm to stop sending marketing messages without valid consent.

For more information: ICO Website

06/19/2026

ICO | Guidance Update | Data (Use and Access) Act 2025

The ICO updated its guidance to reflect that all data protection provisions of the Data (Use and Access) Act 2025 are now in force.

The updated guidance summarizes the DUAA changes affecting organizations using personal information, including amendments to the UK GDPR, Data Protection Act 2018 and PECR. The ICO explains new complaint-handling requirements, including an electronic complaints route, acknowledgement within 30 days and a response without undue delay, alongside changes on automated decision-making, direct marketing, archiving, cookies, children's online services and ICO powers.

For more information: ICO Website

06/15 /2026

UK Government | Proposed Legislation | Introduction of a Social Media Ban

On 15 June, the UK Government announced its intention to introduce new restrictions preventing social media platforms from offering services to children under 16.

The proposal follows Australia's move last year to introduce a similar under-16 social media ban and would require services to deploy highly effective age assurance measures to prevent children under 16 from accessing social media platforms. The Government also announced additional functionality-based restrictions, including restrictions on under-16s using livestreaming features and receiving communications from unknown adults across relevant online services, as well as certain default settings for users aged 16/17. The proposal also includes additional measures for AI chatbot services. In particular, AI "romantic companion" chatbots are expected to be subject to a minimum age requirement of 18, with similar intimate functionalities restricted for under-18s across AI chatbot services more broadly. The new requirements are expected to be implemented through secondary legislation under the Online Safety Act 2023. The Government intends to bring the proposals before Parliament in Q4 2026, with the measures expected to begin coming into force from Q2 2027. Ofcom is also expected to publish a report in October setting out its assessment of age assurance technologies and their application to services used by under-16s.

For more information: UK Government Press Release

06/11/2026

ICO | Guidance | Consumer Internet of Things Products and Services

The ICO published updated guidance for organizations developing and offering consumer IoT products and services.

The guidance covers UK GDPR and PECR issues for consumer IoT products, including accountability, controller and processor roles, lawful basis and consent, fairness where AI is used, transparency in multi-user settings, accuracy, security, privacy-enhancing technologies and data subject rights. The ICO also published its consultation response summary, noting changes on repeated consent requests, embedded third-party services, telemetry and diagnostic data, accessibility, voice ID, generative AI and children's protections.

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, 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)

GIBSON DUNN

gibsondunn.com