View in browser

Privacy, Cybersecurity, and Data Innovation Update

June 15, 2026

European Data Privacy Newsletter

We are pleased to provide you with the May 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

05/26/2026

NIS Cooperation Group | Templates | NIS2 Incident Reporting

The NIS Cooperation Group has adopted common templates for cyber incident reporting under the NIS2 Directive.

The templates were agreed at the Group's 39th plenary meeting in Cyprus by EU Member States, the European Commission and ENISA. They establish a common reporting format and harmonized reporting fields for cybersecurity incident notifications across the EU, with the aim of reducing administrative burden and supporting consistent compliance with NIS2 reporting obligations. The European Commission frames the templates as a first step toward the single-entry point for incident reporting proposed under the Digital Omnibus. As a next step, the European Commission is expected to adopt the templates through an implementing act, making them mandatory for all Member States.

For more information: European Commission [EN]

05/05/2026

European Commission | Cooperation | EU-Japan Digital Platform Regulation Cooperation

The European Commission and Japan's platform regulator have entered into a cooperation arrangement on digital platform supervision.

Signed during the fourth EU-Japan Digital Partnership Council, the arrangement is intended to support supervisory work under the EU Digital Services Act and Japan's Information Distribution Platform Act. According to the European Commission, cooperation will focus on areas of common interest including platform transparency requirements and notice-and-action mechanisms and will be carried out through technical expert dialogues, joint training, the sharing of best practices, joint studies and coordinated research projects.

For more information: European Commission [EN]

France

05/28/2026

CNIL | Guidance | Cloud Computing under the GDPR

The CNIL has published guidance clarifying how GDPR roles should be allocated between cloud providers and their customers.

The guidance examines the qualification of cloud providers and customers as controllers, processors or joint controllers in the context of service provision, service improvement, and cloud security. It states that, for service provision, the customer generally acts as controller and the provider as processor; for security "of" the cloud, the provider may act as controller; and for security "in" the cloud, the customer generally remains controller with provider support as processor. The CNIL further recommends documenting the qualification reasoning where roles are uncertain.

For more information: CNIL Website [FR]

05/27/2026

CNIL | Case Study | Cyberattack at a Processor and Data Breach Response

The CNIL has published a case study on data breach response where a processor is compromised.

The scenario - fictional but based on real incidents notified to the CNIL - describes a cloud solution provider compromised through social engineering, with the attacker copying data belonging to both the provider itself and several of its client companies. The case turns on the provider's dual role: it acts as a controller for its own data and as a processor for its clients' data, and must handle both sets of obligations at once. The CNIL highlights the processor's duty to alert controllers rapidly, the controller's duty to notify the CNIL within 72 hours, and the duty to inform affected individuals where the breach is likely to result in a high risk. It also sets out preventive measures for controllers, DPOs and security teams before outsourcing processing.

For more information: CNIL Website [FR]

05/18/2026

CNIL | Report | 2025 Annual Report and Cybersecurity Enforcement Priorities

The CNIL has published its 2025 annual report and announced a stronger cybersecurity focus for 2026.

The report records 20,150 complaints, 323 investigations, and 259 corrective measures including 83 sanctions, with fines totaling nearly €487 million in 2025. The CNIL also received 6,167 data breach notifications, with hacking accounting for around half of notified incidents, and said it will devote 50% of its controls and enforcement actions in 2026 to data security, including in sectors processing large volumes of sensitive or highly personal data.

For more information: CNIL Website [FR]

Germany

05/06/2026

BfDI | Report | 34th Activity Report

Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI) has presented its activity report for 2025.

The report notes an increase in supervisory activity, with 11,824 submissions received in 2025 (+36% year-on-year), alongside 80 on-site inspections, 40 written audits, and 129 supervisory measures. It also highlights a €45 million fine imposed on a telecommunications company over deficiencies in the supervision of partner agencies and authentication processes. In addition, the BfDI outlines several initiatives launched in 2025, including “ReguLab,” its dedicated data protection sandbox introduced as part of its broader guidance efforts. Finally, the BfDI expresses concerns regarding the proposed reform to the oversight of intelligence services, which would transfer supervisory responsibility from the BfDI to the Independent Control Council (UKRat).

For more information: BfDI Website [DE]

05/04/2026

Berlin DPA | Reprimand | Data Breach at a Public Transport Operator

The Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) reprimanded the Berlin public transport operator over its handling of a data breach at a processor.

The breach arose when a service provider - engaged by the operator to send letters and emails, and handling around 180,000 customer records (names, addresses, contract and customer numbers and, in part, email addresses) - was hit by a cyberattack in 2025. The Berlin DPA found that the operator had relied on the processor’s contractual assurance that the data would be deleted without verifying that deletion had in fact taken place, even though the data should no longer have been stored once the assignment had ended, in breach of Article 5(2) read with Article 5(1)(c), (e) and (f) and Article 32(1) GDPR. It further found that the operator had notified the breach late, contrary to Article 33 GDPR. The authority issued a reprimand rather than a fine. The case underscores that controllers must actively

monitor their processors, including as regards data deletion, and report breaches without undue delay.

For more information: Berlin DPA [DE]

Ireland

05/08/2026

Data Protection Commission | Sanction | Data Breach

The Irish Supervisory Authority (DPC) has published its final decision following an inquiry into a series of personal data breaches at a bank.

The breaches arose after malicious actors used customer information to impersonate customers through the controller's contact center, gain access to their accounts, amend account details, and obtain additional account information. The DPC found infringements of Articles 5(1)(f), 32(1) and 33(1) GDPR, concluding that appropriate security protocols had not been followed in any of the three incidents. The authority reprimanded the bank, fined it €250,000 for security-related infringements and €27,500 for the delayed breach notification.

For more information: DPC Website [EN]

05/05/2026

Data Protection Commission | Inquiry | Transfers of Personal Data to China

Ireland's DPC has opened an inquiry into an online fashion retailer's transfers of personal data to China.

The inquiry concerns transfers of personal data of EU and EEA data subjects from the online fashion retailer's Irish entity to China. The DPC states that the inquiry will assess compliance with GDPR Article 5, Article 13 and Chapter V, with particular focus on whether the transfer arrangements between the Irish company and China ensure a level of protection essentially equivalent to that guaranteed in the EU. The

DPC also indicated that the investigation will be conducted in cooperation with other European supervisory authorities.

For more information: DPC Website [EN]

Italy

05/28/2026

Garante | Warning | AI in the Workplace

The Italian Supervisory Authority (Garante) warned an Italian start-up that its workplace AI tool may violate data protection and worker-protection rules.

The Garante issued a formal warning to a start-up whose AI-powered workplace monitoring tool analyzes employee communications to infer stress levels and emotional states. The Garante stressed that such processing could infringe the GDPR, Italian worker-protection rules, and the EU AI Act's ban on workplace emotion-inference systems and ordered privacy-by-design safeguards to prevent employer access to individual emotional data.

For more information: Garante Website [IT]

05/21/2026

Garante | Sanction | Data Breach

The Garante has reported an €85,000 fine against a consulting firm for GDPR infringements following a data breach.

The breach resulted in unauthorized access to personal data relating to more than 61,000 users of online services, including names, emails, and passwords. The Garante found infringements of Articles 5(1)(e) and (f), 32 and 34 GDPR, noting in particular that certain passwords were stored in clear text or protected with outdated cryptography, and that credentials for unused systems had been retained. The authority also found that affected individuals were informed approximately two

months after the incident was discovered, and only following a corrective order, stressing that reputational concerns cannot override data subjects' rights.

For more information: Garante Website [IT]

05/06/2026

Garante | Press Release | Deepfakes

The Garante has issued a further warning on deepfake services that generate harmful content from real images or voices.

The Garante, in a push to obtain greater powers to deter deepfakes, states that services using AI to generate and share content from real images or voices, including services that "undress" people without consent, may seriously affect fundamental rights and freedoms and may also involve criminal conduct. It recalls an earlier warning concerning AI-based services, and states that the authority should be able to block access from Italy to such services in order to limit rapid viral dissemination of harmful material.

For more information: Garante press release [IT]

The Netherlands

05/08/2026

AP | Sanction | Unlawful Transfers to Russia

The Dutch Supervisory Authority (AP) has fined the operator of a taxi app €100 million for unlawful transfers of personal data from Finland and Norway to Russia.

The AP fined the operator for unlawfully transferring personal data of Norwegian and Finnish drivers and customers to Russian servers, including sensitive data such as ID scans, locations, chat content, and social security numbers. The AP found violations of GDPR after the operator failed to implement adequate safeguards for transfers outside the EEA, noting that Russia's lack of an independent privacy

authority creates risks of government access, and ordered the company to cease all transfers immediately.

For more information: AP Website [NL]

Spain

05/28/2026

AEPD | Guidance | Legal Reports Publication

The Spanish Supervisory Authority (AEPD) has published more than 1,500 of its legal opinions as open data.

The AEPD has made more than 1,500 legal opinions publicly available to promote legal certainty and proactive compliance, covering interpretations of data protection law across multiple sectors. The reports, issued in response to consultations from organizations and individuals, can now be browsed individually or bulk-downloaded via a new Open Data section, advancing the transparency goals of the AEPD's 2025–2030 Strategic Plan.

For more information: AEPD Website [ES]
05/26/2026

AEPD | Decision | Termination of Cross-Border Proceeding

The AEPD has closed a cross-border GDPR proceeding against a travel technology company after voluntary payment of €14.4 million.

The AEPD fined Amadeus €18 million (reduced to €14.4M after voluntary payment) for aggregating travelers' booking data into profiles for product development without adequate transparency under Article 14 GDPR or a valid lawful basis under Article 6. The cross-border investigation found that Amadeus reused years-old booking data from airlines and travel agencies for purposes travelers could not reasonably expect, without providing specific notice or demonstrating a proper legitimate-interest balancing test.

For more information: AEPD Decision [ES]

05/06/2026

AEPD | Annual Report | 2025 Annual Report

The AEPD has reported a significant increase in complaints and continued activity in cross-border cases.

The AEPD's 2025 annual report records 30,931 complaints, a 64% increase compared with the previous year, and notes growth in sanctions and warnings linked to data breaches. The report also highlights 1,118 cross-border cases in which the AEPD participated, 47 cases in which it acted as lead supervisory authority, total sanctions of €48.108 million, and more than 126,000 registered DPOs.

For more information: AEPD Annual Report [ES]

United Kingdom

05/19/2026

ICO | News | Data Protection Complaints Process

The UK's Supervisory Authority (ICO) has reminded organizations that new statutory complaints-handling requirements will apply from 19 June 2026 under the Data (Use and Access) Act 2025.

Under the Data (Use and Access) Act 2025, all UK organizations must have a formal data protection complaints process in place by 19 June 2026, requiring a clear channel for complaints, acknowledgment within 30 days, timely investigation, and communication of outcomes. The ICO is urging SMEs in particular to review its published guidance now, emphasizing that a good complaints process protects customer trust and reduces regulatory risk.

For more information: ICO Website [EN]

05/18/2026

ICO | Advice | Online Advertising Rules

The ICO has published advice to the UK Government on possible amendments to online advertising rules under PECR.

The ICO has published advice to the UK government recommending that PECR Regulation 6 be amended to exempt low-risk, context-based advertising from consent requirements, while maintaining mandatory consent for intrusive cross-site behavioral tracking and profiling. The proposal aims to reduce consent fatigue, incentivize privacy-preserving ad technologies, and remove regulatory barriers to innovation, though current rules remain in force until any legislative change is made.

For more information: ICO Website [EN]

05/11/2026

ICO | Sanction | Cyberattack and Data Breach

The ICO has fined two companies £963,900 (€1,105,453) after a cyberattack affecting more than 633,000 people.

The ICO intervened after a phishing-initiated breach went undetected for nearly two years, ultimately resulting in 4.1TB of personal data, including bank details, National Insurance numbers, and health-related information, being published on the dark web. The investigation revealed critical security failures including minimal network monitoring (only 5% coverage), use of obsolete software like Windows Server 2003, and inadequate access controls, with the ICO stressing that proactive security is a legal requirement, not optional. Accordingly, the ICO identified infringements of Article 5(1)(f) and Article 32(1) UK GDPR, and noted that the companies reached a voluntary settlement, admitted the infringement, and agreed to pay the reduced fine without appeal.

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)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our website.

For information about how we process your personal information and rights you may have with respect to such processing, please refer to our Privacy Statement.
Preferences | Unsubscribe | Forward View online