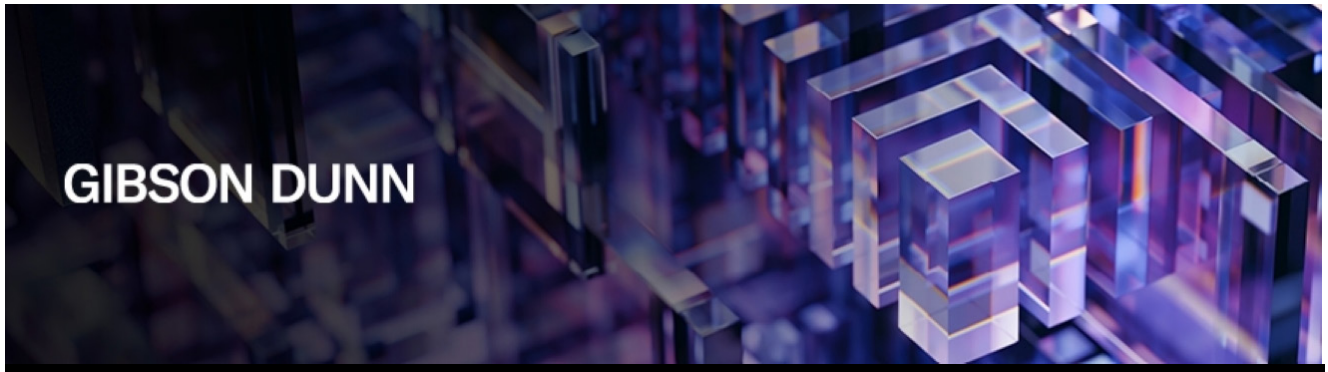
View in browser



Privacy, Cybersecurity, and Data Innovation Update

May 15, 2026

European Data Privacy Newsletter

We are pleased to provide you with the April 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

04/29/2026

European Commission | Recommendation | EU Age Verification App

The Commission has urged Member States to accelerate deployment of the EU age verification solution and make it available by the end of 2026.

Alongside this push targeting EU Member States, the Commission also adopted a Recommendation on age assurance and age verification technologies. The Recommendation indicates that Member States can deploy the solution either as a standalone app or through the future European Digital Identity Wallet. The Commission also states that the app is designed to let users prove tey meet an age threshold without revealing their exact age, identity, or other personal details, and sets out the steps needed to ensure interoperability and swift rollout across the EU.

For more information: European Commission website and Recommendation [English]

04/16/2026

EDPB | Consultation | Personal Data for Scientific Research Purposes

The EDPB has opened a public consultation on draft guidance clarifying how the GDPR applies to scientific research.

The consultation concerns draft Guidelines 1/2026 on the processing of personal data for scientific research purposes. The draft guidance addresses GDPR issues arising in research contexts, including health-related research, the allocation of roles and responsibilities among actors involved in research projects, applicable legal bases (including consent), data subject rights and the conditions under which they may be limited, and expected safeguards when personal data is processed for scientific research. The consultation runs until 25 June 2026 and comments submitted through the consultation form will be published on the EDPB website.

For more information: EDPB Guidelines [English]

04/14/2026

EDPB | Public Consultation | Official DPIA Template

The EDPB has launched a public consultation on a harmonized template intended to promote greater consistency in Data Protection Impact Assessment (DPIA) practices across Europe.

According to the EDPB, the template is designed to help organizations structure, harmonize and evidence their DPIAs and is accompanied by an explainer document addressing practical questions and knowledge gaps. The consultation runs until 9 June 2026, after which supervisory authorities are expected to adopt it either as their own template or as a common "meta-template" compatible with national models; in the meantime, organizations are encouraged to use it and provide feedback as part of the consultation.

For more information: EDPB press release and Public consultation [English]

04/09/2026

EDPB | Report | 2025 Annual Report

The EDPB's 2025 Annual Report highlights a year focused on guidance, regulatory coordination, and practical support for compliance.

The Report underscores the interaction between the GDPR and newer EU digital laws, in particular the DSA, DMA, and AI Act, as well as initiatives on pseudonymization, blockchain, account-creation requirements on e-commerce websites, and coordinated enforcement on the right to erasure. The reported figures include 414 new cross-border cases, 1,299 one-stop-shop procedures, 572 final decisions and approximately €1.16 billion in administrative fines.

For more information: EDPB website [English]

Belgium

04/28/2026

Belgium Supervisory Authority (APD) | Recommendation | Direct Marketing

The APD has overhauled its direct marketing compliance framework through an updated Recommendation and an accompanying practical checklist.

Recommendation 01/2025 adopts a broad understanding of direct marketing and identifies consent and legitimate interest as the main legal bases for the underlying processing activities, while making clear that controllers may not switch legal bases midstream for the same processing purpose. It also addresses sensitive data targeting, processing relating to minors, and the limits of “consent or pay” models. The APD has also published a practical checklist intended to help organizations assess compliance with the framework.

For more information: APD Recommendation and Checklist [French]

04/22/2026

APD / UK Information Commissioner’s Office (ICO) | Memorandum of Understanding | Cooperation Agreement

Belgium’s APD and the UK ICO have signed a Memorandum of Understanding ("MoU") aimed at strengthening cooperation on cross-border data protection issues.

The MoU is framed as a practical cooperation instrument in response to the growing complexity of international personal data flows and seeks to promote more consistent regulatory approaches when both authorities face similar issues. The MoU aims at prioritizing exchange of experience, coordination, and recognition of parallel investigations, while expressly stating that it does not cover any sharing of personal data between the two authorities.

For more information: APD website / MoU [English]

France

04/28/2026

French Supervisory Authority (CNIL) | Guidelines | GDPR Code of Conduct (Retail Sector)

CNIL has approved a new sectoral code for French clothing and footwear retailers.

The code applies to French clothing and footwear retailers that are members of the Alliance du Commerce and act as controllers in consumer retail sales and distribution, both online and in-store. According to the CNIL, this is the first code of conduct of national scope and the third sector-specific code approved by the authority. The code translates GDPR requirements into a practical compliance framework tailored to the retail sector. Only retailers whose decision-making center is located in France, or which constitute a French establishment of an international group, may adhere to the code.

For more information: CNIL website and Code of Conduct [French]

04/27/2026

CNIL | Compliance Tool | Data Protection Officer (DPO)

CNIL has published a practical template to help DPOs structure and present their annual activity reports.

While the CNIL notes that DPO activity reports are not mandatory, it considers them best practice for supporting accountability and monitoring data protection compliance over time. According to the CNIL, such reports can help organizations assess their level of GDPR maturity, report internally on compliance actions and priorities, and strengthen both internal and external communication regarding compliance efforts. The template is therefore intended as a practical accountability tool designed to support the DPO's visibility, governance, and follow-up on compliance actions.

For more information: CNIL website [French]

04/14/2026

CNIL | Recommendation | Tracking Pixels in Emails

CNIL has finalized its Recommendation on the use of tracking pixels in email communications.

The Recommendation emphasizes transparency obligations relating to the use of tracking pixels and recalls that some uses, especially marketing-related ones, require prior consent. This guidance is designed to increase transparency of email tracking, requiring that information be provided in an accessible, understandable and timely manner, and stressing that refusing or withdrawing consent should be as easy as granting it.

For more information: CNIL website and Recommendation [French]

04/07/2026

CNIL | Work Program | 2026 Guidance Roadmap

CNIL has laid out its 2026 guidance work program, outlining upcoming initiatives on consent, AI, health data, access rights, and cybersecurity.

The program includes work on multi-property consent mechanisms, AI deployment in the workplace and the healthcare sector, automatic analysis of voice communications, documentation tools for DPOs, and the allocation of responsibilities across the AI value chain. The CNIL also announced future guidance relating to social housing, health-research methodologies, employees' access right requests, electronic voting, secure messaging, remote identity verification, web-filtering gateways, and endpoint detection and response solutions. The publication shows a clear effort to provide regulated actors with greater visibility over CNIL's upcoming guidance priorities.

For more information: CNIL website [French]

04/03/2026

CNIL | Control Agenda | 2026 Inspection Priorities

The CNIL has announced its 2026 priority inspection themes, with a strong focus on recruitment practices, use of the national electoral register and data processing by sports federations.

The CNIL explains that approximately 20% of its annual inspections are tied to priority themes selected because of their significance for individuals' rights and freedoms. In 2026, it will examine compliance with its 2023 recruitment guidance, especially on automated decision-making, candidate information, and retention periods, with a focus on large companies and recruitment firms. It will also scrutinize uses of the national electoral register and assess sports federations' processing of large volumes of personal data, including health data and data relating to criminal offenses, concerning a significant number of minors, with particular attention to data relevance, retention and security in a sector recently affected by cyberattacks. Additionally, under the 2026 *coordinated enforcement framework*, the CNIL (in coordination with the EDPB) will join other EEA authorities in assessing the transparency and completeness of information provided to data subjects.
For more information: CNIL website [French]

04/02/2026

CNIL | Reference Framework | Retention Periods for Human Resources

CNIL has issued a new practical framework to help employers define retention periods for HR-related data.

The framework applies to private and public employers subject to French labour law and is designed to help employers determine the appropriate retention periods for personal data processing in the context of common HR activities. It covers recruitment, administrative personnel management, payroll, workplace security, professional vehicles, recorded phone calls at work, collective labour relations, workplace accidents, litigation, and whistleblowing. While not legally binding, this framework provides operational guidance and consolidates both soft-law recommendations and retention periods that are mandatory under applicable legislation or regulation.

For more information: CNIL website and Reference Framework [French]

Germany

04/24/2026 and 04/13/2026

Bavarian Data Protection Commissioner (BayLfD) | Guidance | LLM Chatbots and AI Translation Tools

The BayLfD has published practical guidance for Bavarian public bodies on the use of LLM-powered chatbots, following earlier guidance on AI-based translation tools.

The chatbot guidance covers key considerations for procurement, implementation, data processing agreements and DPIAs, as well as technical safeguards such as disabling the use of user inputs for training purposes. The translation-tool guidance focuses on issues such as the processing of voice data, potential biometric data as well as translation accuracy.

For more information: BayLfD chatbot guidance and BayLfD translation guidance [German]

04/22/2026

German Federal Government | Draft Law | IP Address Retention and Law Enforcement Access to Traffic Data

The German Federal Government has approved a draft law that would require internet access providers to retain IP addresses for a period of three months.

According to the government, the proposal is intended to strengthen the investigations and prosecution of online crime. It would also introduce a preservation order enabling law enforcement authorities to preserve traffic data for up to three

months in specific cases. The draft also expands location/cell-site data inquiries to offences of significant importance.

For more information: Federal Government article [German]

04/07/2026

Germany's Cyber Agency (BSI) | Cybersecurity Standard | Secure Cloud Computing

BSI has released the new version of its cloud-security catalogue.

According to the BSI, C5:2026 updates Germany's main security standard for cloud providers and users and translates complex security requirements into auditable criteria. It highlights new treatment of topics such as container management, post-quantum cryptography, and confidential computing. The revised structure is intended to improve usability, comparability, and integration into governance, risk, and compliance processes. The catalogue is closely aligned with the European cloud certification framework and also takes into account ISO/IEC 27001:2022, the CSA Cloud Controls Matrix v4, and the NIS 2 Directive.

For more information: BSI press release [German]

04/02/2026

Administrative Court Düsseldorf | Judgment | GDPR

Administrative Court (VG) Düsseldorf has issued a decision on the requirements for email security under Art. 32 GDPR.

The Court held that the GDPR does not impose a general obligation to use end-to-end encryption for e-mail communication. Rather, the appropriate security measures under Article 32 GDPR must be determined on a risk-based, case-by-case basis, taking into account the specific risks posed to the data subject. In the case at hand, the personal data concerned was not considered particularly sensitive, and encryption during transmission was therefore deemed sufficient to ensure an appropriate level of protection. The Court nevertheless emphasized that stricter measures may be required where the sensitivity of the data or the level of risk is higher.

For more information: Judgment Administrative Court Düsseldorf [German]

04/02/2026

Independent federal and state data protection authorities | Statement | Digital Investigative Powers

The German Data Protection Conference (DSK) has raised concerns about proposed legislation that would expand digital investigative powers, particularly biometric online identification and automated data analysis.

According to the DSK, the draft legislation in its current form poses significant risks to fundamental rights, as it could allow identification and extensive analysis of individuals not involved in criminal conduct. The proposed measures could enable far-reaching surveillance, including by cross-referencing internet data and using AI-based tools to analyze large datasets. The DSK therefore calls for clearer statutory limitations, a stronger focus on proportionality, and more robust safeguards for fundamental rights.

For more information: German Federal Government announcement and DSK press release [German]

Italy

04/21/2026

Garante | Guidelines | Tracking Pixels in Emails

Garante has drawn a clear consent-first framework for tracking pixels used in emails.

According to the Guidelines, tracking pixels generally fall within the same legal framework as cookies and similar tracking technologies, meaning their use requires prior, free, specific, and informed consent. The Garante also identified limited exceptions, such as security or strictly necessary technical uses, while stressing proportionality, data minimization, privacy by design and by default, and the availability of simple withdrawal mechanisms. Providers will have six months from publication in the Official Gazette to comply. While the Garante and the CNIL align on core principles, their guidance differs in several respects, meaning organizations operating across jurisdictions will need to ensure compliance under both regimes.

For more information: Garante Guidelines [IT]

04/20/2026

Garante | Sanction | Two companies fined €12.5 Million

Garante has issued major fines against two companies over unlawful data processing linked to banking service apps.

The Garante issued one of the period's most significant privacy fines – totaling about €12.5 million (€6.624 million and €5.877 million) against two companies providing banking apps. The authority found that the companies had unlawfully processed the personal data of millions of users through invasive device-monitoring measures

embedded in their apps. According to the Garante, users were effectively forced to accept such monitoring measures to access the services. The investigation also identified shortcomings in the information notices, DPIA, retention framework, security measures, and processor arrangements. In addition to the fines, the Garante ordered the companies to stop the unlawful processing (if it had not already ceased) and to bring retention practices into line with its prescriptions.

For more information: Garante's website and decision [IT]

The Netherlands

04/21/2026

Dutch Supervisory Authority (AP) | Public Consultation | Explanations for Automated Decision-Making

AP has opened a consultation on practical tools for explaining automated decisions to individuals.

The AP is developing guidance to help organizations explain automated decision-making in a way that works in practice, as part of its 2026 work on the "right to explanation" in cases where automated decisions have significant consequences for individuals. In substance, the consultation focuses on the information that individuals should receive when such decisions are made about them, including the use of automated decision-making, the significance and likely effects of the decision, the underlying logic, and the rights available to seek human intervention or otherwise challenge the outcome.

For more information: AP website [English]

04/16/2026

AP | Supervisory Initiative | Incoming Preventive Checks on ICT Suppliers

The AP introduces preventive inspections of ICT suppliers as part of its broader cyber-risk supervision strategy.

The AP indicates that the initiative aims to strengthen prevention against cyberattacks and data leaks by assessing in advance how organizations, especially ICT suppliers, have organized their digital security. The AP notes that ICT suppliers often process large volumes of personal data on behalf of many client organizations, meaning that a single breach can have significant downstream effects. The inspections are therefore presented as a preventive measure to help organizations identify and remedy weaknesses before incidents occur.

For more information: AP website [NL]

04/02/2026

AP | Report | 2025 Annual Report

The AP's 2025 annual report reflects an increasingly strategic and intervention-focused approach to supervision.

The authority identifies five priority areas: algorithms and AI, big tech, data trade and leaks, freedom and security, and digital government. It also highlights more frequent use of informal and corrective measures alongside formal enforcement, with 13,517 complaints and 44,374 data breach notifications reported in 2025. The report further notes the AP's expanding role under several EU digital regulations, including the DSA and the Political Advertising Regulation, as well as its broader involvement in EDPB work.

For more information: Autoriteit Persoonsgegevens website [NL]

Poland

04/02/2026

Ministry of Digital Affairs | Cybersecurity | NIS 2 Transposition enters into force

Poland's revised cybersecurity framework has entered into force, triggering the first compliance deadlines for in-scope entities under NIS 2.

The amended Act aligns Poland's national framework with the NIS 2 Directive, expands the range of regulated entities, and introduces new obligations linked to registration, incident reporting, governance, and auditing.

For more information: Ministry of Digital Affairs (Poland) website [Polish]

United Kingdom

04/16/2026

UK Government | Regulations | ICO Code of Practice on AI and Automated Decision-Making

The UK has adopted regulations requiring the ICO to prepare a code of practice on AI and automated decision-making.

The Regulations were made on 16 April 2026, laid before Parliament on 21 April 2026, and came into force on 12 May 2026. They require the ICO to prepare a code

of practice on good practice in the processing of personal data under the UK GDPR and the Data Protection Act 2018, excluding Part 4 of the Act, in relation to developing and using artificial intelligence and automated decision-making; the code must also include guidance on the processing of children's personal data.

For more information: UK Regulations and Legislative history [English]

04/21/2026

National Cyber Security Centre (NCSC) | Guidance | Cross-Domain Guidance for High-Risk Environments

The NCSC has updated its cross-domain architecture guidance to reflect more hostile threat models and more complex connected systems.
The guidance is aimed at organizations operating where targeted attack is assumed and the consequences of compromise are severe, including critical infrastructure and environments holding sensitive information or significant intellectual property. It shifts the focus from fixed boundaries and product-specific controls toward end-to-end architecture, "zones of trust," and function "pipelines" across trust zones; for new end-to-end architectures it largely replaces the older cross-domain security principles, while the original import/export design patterns are being deprecated and further implementation material is awaited.

For more information: NCSC press release / guidance [English]

04/29/2026

ICO | Guidance | Use of Storage and Access Technologies

The ICO has published an updated guide to use of storage and access technologies, following two consultations on draft guidance between 2024 and 2025.

The guidance includes two new chapters on PECR guidance, focusing on (i) the 'simple means of objecting' (clarifying that a simple means of objection could be provided through an existing consent mechanism or use toggles) and (ii) using 'the same storage and access technology for multiple purposes'.

For more information: ICO website [English]

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)