



GIBSON DUNN

Privacy, Cybersecurity, and Data Innovation Update

17 July 2025

European Data Privacy Newsletter

June 2025

Europe

06/26/2025

[ENISA | Guidance | NIS 2 Support Documents](#)

ENISA has released two guidance documents to assist companies in complying with the NIS 2 Directive.

The first document provides non-binding guidance to relevant entities on how to implement the requirements for the cybersecurity risk management measures by providing examples. The second document clarifies the organizational steps to take (including what roles and skills are needed internally) to implement NIS 2 obligations, such as cybersecurity risk measures, post-incident response and reporting.

For more information: ENISA Website [link](#) and [link](#)

06/26/2025

[European Data Protection Board \(EDPB\) | Opinion | Draft Guidelines on Minors Under DSA](#)

The EDPB provided preliminary comments on the European Commission's draft guidelines under Article 28 of the Digital Services Act (DSA), that aim at enhancing online protection for minors.

The Board welcomed the initiative, noted the draft provides clear and practical recommendations on what measures to take to improve minor safety (including privacy) but also called for clarification of the material scope of Article 28. It also mentioned that it intends to provide additional guidance on data protection compliance in the context of its "Children's guidelines" and reiterated its readiness to advise on age assurance and related data protection issues within the Digital Services Board's Working Group 6.

For more information: [EDPB Website](#)

06/24/2025

[European Commission | Adequacy Decision | UK](#)

The European Commission has extended the UK's adequacy decision under the GDPR until December 27, 2025.

As a reminder, the UK Government introduced on October 23, 2024, the Data (Use and Access Bill) which amends the UK GDPR and Data Protection Act 2018. The extension allows the European Commission to assess whether the UK continues to provide an adequate level of protection, pending the outcome of the legislative process.

For more information: [European Commission Website](#)

06/16/2025

[Council of the EU/European Parliament | Agreement | Cross-Border GDPR Enforcement](#)

The Council of the European Union and the European Parliament reached a provisional agreement on a new legislative proposal aimed at improving cooperation among national data protection authorities in cross-border enforcement of the GDPR.

The proposed regulation includes clearer procedural rules for handling cross-border cases, with the goal of streamlining investigations and enhancing the efficiency of cooperation mechanisms between supervisory authorities.

For further information: [European Council Website](#)

06/05/2025

[European Data Protection Board | Guidelines | Data Transfers](#)

The European Data Protection Board (“EDPB”) published the final version of its guidelines regarding data transfers to third country authorities.

The new guidelines aim to provide clarification on Article 48 of the GDPR, outlining how organizations should assess whether and under what conditions they may lawfully respond to requests for the transfer of personal data from authorities in third countries.

For more information: [EDPB Website](#)

06/05/2025

[European Data Protection Board | Report | AI and Data Protection](#)

The European Data Protection Board (“EDPB”) published two reports providing training material on AI and data protection.

The first report, “Law & Compliance in AI Security & Data Protection”, is tailored for privacy and data protection professionals, such as DPOs, while the second report, “Fundamentals of Secure AI Systems with Personal Data”, is designed for technically oriented professionals, including cybersecurity experts and developers.

For more information: [EDPB Website](#)

06/04/2025

[European Union Agency for Cybersecurity | Update | National Cybersecurity Strategies](#)

The European Union Agency for Cybersecurity (“ENISA”) updated its National Cybersecurity Strategies (“NCSS”) Interactive Map.

The NCSS Map serves as a platform offering insights on how EU Member States implement their cybersecurity strategies, highlighting their objectives, actions and best practices.

For more information: [ENISA Website](#)

Belgium

06/26/2025

[Belgian Supervisory Authority | Procedural Decision | Dismissal of NOYB Complaints](#)

The Belgian Supervisory Authority (“APD”) dismissed 16 complaints across 5 cases filed by NOYB, citing the prohibition of abuse of rights under GDPR.

The APD found that NOYB had instructed complainants on how to grant mandates for filing complaints, without properly representing the individual data subjects. The ADP recalled that in the European Union, including Belgium, associations cannot file complaints in their own name, but only as representative acting on the basis of a mandate from the data subject.

For more information: [APD Press release](#) [FR]

France

06/19/2025

[French Supervisory Authority | Recommendations | AI and Legitimate Interest](#)

The French Supervisory Authority (“CNIL”) published new recommendations on the use of legitimate interest in the development of AI systems.

The CNIL outlines the conditions which legitimate interest may be relied upon, in particular in the context of web scraping. These recommendations are intended to help stakeholders assess when legitimate interest can be used as a legal basis. The recommendations also provide concrete examples of data processing activities that may be justified on the grounds of legitimate interest.

For more information: [CNIL Website](#) [FR]

06/12/2025

[French Supervisory Authority | Public consultation | Tracking Pixels](#)

The French Supervisory Authority (“CNIL”) launched a public consultation on a draft recommendation on tracking pixels, aimed at clarifying the legal framework for their use in emails and on websites.

The draft recommendation outlines requirements related to user consent, information obligations, and data sharing with third parties. Stakeholders can submit feedback until 24 July 2025.

For more information: [CNIL Website](#) [FR]

06/10/2025

[French Supervisory Authority | Recommendations | Workplace Diversity Surveys](#)

The French Supervisory Authority (“CNIL”) published recommendations on the conduct of internal diversity surveys in the workplace.

These non-binding guidelines aim to help organizations collect sensitive personal data securely and in a way that respects individuals’ privacy rights and the GDPR through measures such as voluntariness, clear information, data minimization, and strong safeguards like anonymization or pseudonymization.

For more information: [CNIL Website](#) [FR]

06/06/2025

[French Supervisory Authority | Guidance | Roles of Controllers and Processors](#)

The French Supervisory Authority (“CNIL”) published a guidance on the roles of data controllers and data processors.

This guidance stresses that all parties in data processing must clearly define and document their roles based on actual responsibilities as misclassification can jeopardize GDPR compliance and lead the CNIL to reclassify roles during audits, possibly resulting in sanctions.

For more information: [CNIL Website](#) [FR]

Germany

06/17/2025

[Data Protection Conference | Guidance | AI Systems and Data Protection](#)

The Data Protection Conference of the German Supervisory Authorities (DSK) published an orientation guide outlining key data protection requirements for the development and use of AI systems, in particular regarding the required technical and organizational measures.

The guidance highlights the need for appropriate technical and organizational measures (TOMs) to mitigate risks, especially in high-risk processing scenarios. The document is intended to support both public and private sector actors in aligning AI deployment with fundamental rights and data protection standards.

For more information: [DSK Website](#) [DE]

06/16/2025

[Data Protection Conference | Resolution | Confidential Cloud Computing](#)

The Data Protection Conference of the German Supervisory Authorities (DSK) published a resolution on “confidential cloud computing”.

The resolution acknowledges that various diverse definitions of "confidential cloud computing" exist. It emphasizes, that confidential cloud computing may significantly enhance overall protection levels - especially against other cloud users and certain insider threats. As part of a "defense-in-depth" strategy, it provides valuable additional layers of security, even if absolute confidentiality from the cloud provider cannot be guaranteed. Clear attacker models and transparent documentation of implemented measures are essential prerequisites.

For more information: [DSK Website](#) [DE]

06/16/2025

[Data Protection Conference | Guideline | Procedure on Fines of Data Protection Supervisory Authorities](#)

The German Data Protection Conference (DSK) has adopted model guidelines for the conduct of administrative fine proceedings by data protection supervisory authorities.

The DSK aims to establish nationwide standards for supervisory authorities and how to handle fining procedures under the GDPR. The guidelines define procedural principles, responsibilities, cooperation obligations of the parties involved, and the methodology for calculating and

assessing fines. They are intended to enhance transparency and legal certainty for both organizations and individuals, while also promoting consistency in enforcement practices.

For more information: [DSK Website](#) [DE]

06/10/2025

[German Federal Supervisory Authority | Sanctions | Telecommunication Company](#)

The German Federal Supervisory Authority has fined a telecommunication company a total of €45 million following investigations into its partner agencies and online service portal.

More specifically, a €15 million fine was imposed for insufficient supervision and auditing of partner agencies processing customer data. A €30 million fine was imposed for weak authentication procedures that could allow misuse of eSIMs via the hotline when used in combination with the Company's online portal. A reprimand was also issued in relation to identified IT system vulnerabilities.

For more information: [EDPB Website](#)

06/10/2025

[North Rhine-Westphalia Supervisory Authority | Activity Report](#)

The North Rhine-Westphalia Supervisory Authority (LDI NRW) published their annual activity report.

The North Rhine-Westphalia Supervisory Authority has voiced opposition to the government's plan to centralize data protection at the federal level, highlighting the importance of regional data protection authorities.

For more information: [LDI NRW Website](#) [DE]

Greece

06/11/2025

[Hellenic Supervisory Authority | Decision | EU Representative](#)

The Hellenic Supervisory Authority published a decision of May 2025 ordering a Chinese-based provider of a large language model (LLM) to appoint an EU representative, pursuant to Article 27 of the GDPR.

The Authority considered that the company targets EU data subjects, notably in Greece, through web and mobile services available in Greek, and failed to provide a compliant privacy policy or lawful basis for processing.

For more information: [Hellenic Authority Website](#)

Slovenia

06/04/2025

[Slovenian Government | Publication | NIS II](#)

The Information Security Act (“ZInfV-1”) transposing the NIS II Regulation was published in the official gazette of the Republic of Slovenia.

The Information Security Act will enter into effect on June 19, 2025.

For more information: [Slovenian Government Website](#) [SI]

United Kingdom

06/19/2025

Royal Assent | Data Use and Access Act | GDPR & PECR Update

The Data (Use and Access) Act (“DUUA”) received Royal Assent.

The DUUA updates certain aspects of data protection and e-privacy law, aiming to facilitate the safe and effective use of data, encourage innovation, simplify data protection compliance requirements for organisations and align the PECR enforcement regime to that under UK GDPR. The Act amends and supplements the UK GDPR, the DPA 2018 and PECR.

For more information: [ICO Website](#)

06/17/2025

Information Commissioner’s Office | Fine | Genetic Data

ICO fines 23andMe £2.31 million for failing to have appropriate security measures in place and to protect UK users’ genetic data.

The penalty results from a joint investigation conducted by the ICO and Canada Privacy Commissioner (“CPC”), after 23andMe failed to protect UK users' personal data during a major 2023 cyber-attack. In particular, 23andMe did not have mandatory MFA, secure password protocols, unpredictable usernames, and effective systems in place to monitor, detect, or respond to cyber threats. It also failed to have adequate controls over access to raw genetic data.

For more information: [ICO Website](#)

06/16/2025

Information Commissioner’s Office | Guidance | IoT

ICO publishes draft guidance on Internet of Things (“IoT”) products.

The ICO's draft guidance is intended to support IoT developers (e.g. of smart home appliances and wearable tech) with their data protection compliance. The guidance sets clear expectations on how to do so, addressing for instance how to request informed consent or provide transparent privacy information.

For more information: [ICO Website](#)

06/05/2025

[Information Commissioner's Office | Guidance | AI and Biometrics Strategy](#)

The Information Commissioner's Office ("ICO") published its AI and biometrics strategy.

This new AI and biometrics strategy aims at ensuring organisations are developing new technologies lawfully, while supporting innovation.

For more information: [ICO Website](#)

06/04/2025

[National Cyber Security Centre | Guidance | Cyber Security Culture Principles](#)

The National Cyber Security Centre ("NCSC") launched its Cyber security culture principles.

The guidance aims at helping professionals in supporting a cyber secure organization.

For more information: [NCSC 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, Clémence Pugnet, 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)
Timothy W. Loose – Los Angeles (+1 213.229.7746, tloose@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@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)
Benjamin B. Wagner – Palo Alto (+1 650.849.5395, bwagner@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)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@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.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our [website](#)