



GIBSON DUNN

Privacy, Cybersecurity, and Data Innovation Update

October 13, 2026

European Data Privacy Newsletter

We are pleased to provide you with the September 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

09/17/2026

[EDPB | Guidelines | Imposition of Administrative Fines](#)

The EDPB adopted guidelines on how supervisory authorities should decide whether to impose an administrative fine, on its own or alongside the other corrective measures provided for in Article 58(2) GDPR, with a view to harmonizing fining practice across the EU.

These guidelines complement Guidelines 04/2022 on the calculation of administrative fines and are intended to replace the earlier guidance of the Article 29 Working Party. They set out a methodology in five steps. The first three steps cover the legal preconditions for a fine; the fourth step relates to the factors listed in Article 83(2) GDPR; and in the fifth step, it should be assessed whether a fine would be effective, proportionate and dissuasive in the individual case, and may deviate from the general approach in either direction. The guidelines also contain 14 practical

examples. The guidelines are subject to public consultation until 13 November 2026, and their methodology will be subject to regular review by the EDPB. For more information: [EDPB website](#) and [Guidelines](#)

09/17/2026

[EDPB | Guidelines | Interplay between the DSA and the GDPR](#)

The EDPB adopted the final version of its guidelines on the interplay between the DSA and the GDPR, which clarify how intermediary service providers should apply the GDPR when processing personal data to comply with their obligations under the DSA.

The guidelines cover the DSA provisions that interact most closely with the GDPR. They clarify when compliance with a legal obligation or legitimate interests can serve as a lawful basis for measures to detect, identify and disable illegal content. On the protection of minors, Articles 28(1) and (2) DSA can qualify as a legal basis under Article 6(1)(c) GDPR where the processing is necessary and proportionate.

Providers should also avoid age assurance mechanisms that allow users to be identified unambiguously online.

For more information: [EDPB website](#) and [Guidelines](#)

09/17/2026

[European Commission | Proposal | EU KIDS Act](#)

The European Commission has proposed the EU KIDS Act ("Keeping Internet Digital Spaces Accountable and Trustworthy"), which would introduce gradual, age-based access to social media for children and impose safety obligations on online services used by minors across the EU.

The proposal will apply to online services used by minors, including social media, video sharing platforms, online games, AI companions and chatbots. Under the proposal, children under 13 will not be able to access social media services, while children aged 13 to under 15 will be able to use a mini account managed by a parent or guardian, with limited features and a time restriction of 1 hour per day. From age 15 onwards, they will be able to open and manage their own account. Services covered by the proposal will also have to limit features that encourage excessive use, prohibit unsolicited contact from strangers and make minors' profiles private by default. The proposal will now be examined by the European Parliament and the

Council.

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

France

09/10/2026

CNIL | Guidance | Electronic Invoicing

The CNIL published guidance on the personal data protection issues raised by the electronic invoicing reform for business-to-business transactions, the first phase of which entered into force on 1 September 2026.

The CNIL recalls that data protection rules only apply to the data of natural persons and not of legal persons, and that particular attention must be paid to the data minimization principle where invoice fields are customized. The company issuing or receiving the invoices acts in principle as a controller, while the approved platform acts as a processor, unless it reuses the data for its own purposes. The ten-year legal retention period for accounting documents applies to electronic invoices. Approved platforms must be ISO 27001 certified and, where applicable, rely on a SecNumCloud qualified solution. The CNIL warns that these requirements are not necessarily sufficient to ensure compliance with the security obligation of Article 32 GDPR.

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

09/09/2026

CNIL | Sanction | Right to Erasure of Personal Data

The CNIL issued a sanction of 300.000 euros against an IT consulting company for several breaches relating to the respect of individuals' rights, in particular the right to erasure.

In 2024, the CNIL received several complaints from former employees or candidates relating to the difficulties encountered in exercising their right to erasure. In the context of its investigations, the CNIL noted that, out of the 265 erasure requests received by the company, more than three quarters had not been handled or had not been handled satisfactorily. The CNIL also found that the company had failed to comply with its obligation to inform the data subjects of the action taken on their erasure requests. The fine imposed takes into account in particular the disregard of

essential principles relating to the rights of individuals and the fact that the company had already been reminded of its obligations on two occasions.

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

09/03/2026

CNIL | Sanction | Health Data Violation

The CNIL issued a sanction of 500.000 euros against a hospital for not having taken appropriate measures to ensure the security of its patients' and some of their relatives' data.

Following a data breach in the summer of 2025 that led to unauthorized access to the data of 524.867 patients and 202.246 people designated as "trusted third parties", the CNIL carried out an audit which highlighted several breaches by the hospital. The CNIL found that the entity had not implemented certain basic security measures that could have made the attack more difficult and that the security measures deployed to ensure the confidentiality of the data were not sufficient. The CNIL also found that the affected patients were informed of the data breach, but no direct information had been provided to the individuals designated by patients as trusted third parties. The fine imposed takes into account in particular the disregard of essential security principles, the number of individuals affected, the nature of the compromised data and the financial capacity of the entity.

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

Germany

09/30/2026

BfDI | Working Paper | Confidential Cloud Computing

The Berlin Group, the international working group on data protection in technology led by the BfDI, has presented a new paper with recommendations on confidential cloud computing.

The Berlin Group recommends the use of confidential computing in cloud environments, as this technology can increase security and data protection. After an introduction to the technology and its use in cloud computing, the paper addresses specific data protection aspects. It sets out the benefits but also the limits of this

technology. Finally, it contains key recommendations for the use and development of such products in order to effectively strengthen data protection.

For more information: [BfDI website](#) [DE]

09/24/2026

DSK | Short Papers | Updated Guidance on Consent and on Supervisory Powers and Sanctions

The DSK published updated versions of its short papers No. 20 on consent and No. 2 on supervisory powers and sanctions.

The updated short paper No. 2 incorporates a CJEU judgment, under which a fine may be imposed directly on an undertaking for any culpable infringement committed by persons acting on its behalf, without the need to attribute the infringement to the conduct of a legal representative as previously required under Section 30 of the German Administrative Offences Act (OWiG). As regards the calculation of fines, the statutory maximum is to be determined on the basis of the group's worldwide turnover, and the DSK refers to the five-step methodology of the EDPB Guidelines 04/2022 as the applicable framework. The DSK stresses that a fine may be combined with other corrective measures where this is necessary and proportionate.

Short paper No. 20 reflects the EDPB Guidelines 05/2020 and the CJEU's and BGH's cookie case law: pre-ticked boxes, silence or merely continuing to use a service do not constitute consent. In addition, "consent or pay" models are only voluntary if the alternative offered without tracking is genuinely equivalent. The DSK further stresses that controllers must document each individual consent.

For more information: [Short Paper No. 2](#) and [Short Paper No. 20](#) [DE]

09/17/2026

BGH | Referral | Household Exception under the GDPR

The BGH has referred questions to the CJEU to clarify the conditions of the so-called "household exception" under Article 2(2)(c) GDPR.

Under this exception, the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. The first case concerns the forwarding of private chat messages to the office manager of the medical practice where the claimant worked. The second case concerns the video surveillance of a kitchen-living room and the forwarding of the recordings to the police. In both cases, the courts of appeal held that the GDPR did not apply because of the household exception. The CJEU is asked in particular how the notions of

"personal" and "household" activities should be understood and whether the purpose of the processing must be taken into account.

For more information: [BGH website](#) [DE]

09/10/2026

Lower Saxony DPA | Statistics | Rise in Reported Data Breaches

The Lower Saxony Data Protection Commissioner reported a sharp increase in personal data breach notifications, with 1,245 notifications in the first half of 2026 – an increase of 58%.

As the trend continued over the summer, the authority has already received more notifications in 2026 than in the whole of 2025. Most cases concerned misdirected mailings and accidental disclosures but cyberattacks through hacking and phishing are also increasing. The authority recommends two-factor authentication, automated and clearly defined processes, the four-eyes principle when sending sensitive data and regular staff training.

For more information: [LfD Niedersachsen website](#) [DE]

Ireland

09/25/2026

DPC | Report | Supervision of Artificial Intelligence

The DPC published a report on its supervision of AI products and services between 2021 and 2025, highlighting its engagement with around 180 AI systems, including large language models, facial recognition and AI agents.

The report identifies lawful basis, transparency and data minimization as key compliance issues, notes improvements secured through regulatory engagement, and emphasizes that early engagement with regulators is the most effective route to compliant AI innovation.

For more information: [DPC website](#) and [Report](#)

Netherlands

09/03/2026

[AP | Practical Templates | Processing Register and Privacy Statement](#)

The AP has published two practical templates for a processing register and a privacy statement, in particular for SMEs.

The templates contain sample tables for ten sectors such as education, hospitality, retail, IT and logistics, so that businesses only have to remove what does not apply to them and complete the information where necessary. The AP indicates that the information contained in the processing register can be used when drawing up the privacy statement and processor agreements and when giving effect to the privacy rights of data subjects. The AP adds that, in the future, a processing register may only have to be kept where the processing operations present a high privacy risk, as proposed by the European Commission.

For more information: [AP website](#) [NL]

Norway

09/21/2026

[Datatilsynet | Inspection | Security of Hotel Booking Processes](#)

The Norwegian data protection authority (Datatilsynet) has launched an inspection of the hotel sector focusing on the security of personal data in booking and reservation processes.

Over time, the Datatilsynet has received a number of breach notifications, complaints and tips about security breaches. They concern systematic fraud attempts targeting customers after hotel bookings, across several hotels and chains. Personal data has therefore ended up in the wrong hands and its misuse may have negative consequences for the persons affected. The Datatilsynet intends to map the extent and causes of these fraud attempts. It will also examine whether the hotel chains have implemented sufficient technical and organizational measures to ensure a level of security in line with data protection requirements. The inspection will take place in two phases. A written inspection comes first, followed later this year by on-site inspections at selected hotels.

For more information: [Datatilsynet website](#) [NO]

Poland

09/29/2026

UODO | Intervention | Data Leak from Online Platform

The Polish data protection authority (UODO) has asked the Prosecutor General to reopen the criminal proceedings concerning a data leak affecting up to 1.3 million customers of a Chinese online sales platform.

The leak concerned customers of the platform, including several tens of thousands of people in Poland. The data included names, email addresses, telephone numbers, IP addresses, passwords, delivery addresses, as well as order and payment details. In April 2024, an interactive map of Poland showing the names and delivery addresses of customers was published on several websites. The UODO reported a suspected criminal offense, but the prosecutor's office refused to open an investigation and later discontinued the proceedings. The UODO considers that the evidence was not examined comprehensively and that the perpetrators have not been identified.

For more information: [UODO website](#) [PL]

09/25/2026

UODO | Inspection | Medical Data Leak

Following media reports of a new leak that may concern the medical data of up to five million Poles, the UODO has announced an inspection of a healthcare software vendor.

The incident results from an attack on the healthcare software. The Central Cybercrime Bureau is investigating the case. According to the Minister of Digital Affairs, the company had not yet reported the incident to competent cybersecurity teams. The UODO took similar action in August after the leak of data from another healthcare software vendor which related to 19 million Poles. By 17 September, the UODO had received more than 50 complaints and reports about the August incident, as well as over 2,000 notifications from controllers. In view of this attack and many other breaches, the UODO decided on 16 September that wider inspections of the processing of health data were needed. It therefore announced additional inspections until the end of 2026.

For more information: [UODO website](#) [PL]

Spain

09/28/2026

[AEPD | Publication | Offensive AI and Data Protection](#)

The Spanish Data Protection Agency (AEPD) warns that cybercriminals use artificial intelligence, particularly AI agents, to accelerate cyberattacks, reduce intrusion times and exploit vulnerabilities in an automated way.

The AEPD notes that data breach notifications have increased by 150% in 2026 compared to 2025. In the short term, it suggests a risk analysis focused on the rights and freedoms of natural persons, a Zero Trust approach, resistant multi-factor authentication and least privilege access. Organizations should also minimize their exposure to the internet, purge data outside the retention period and ensure the ability to restore data, processes and services. In the long term, the AEPD calls for real governance of digital technologies, a strengthened record of processing activities and strict data minimization.

For more information: [AEPD website](#) [ES]

09/22/2026

[AEPD | Sanction | Exercise of Data Subject Rights](#)

The AEPD fined a security alarm and video-surveillance company 100,000 euros for making the exercise of data subject rights more difficult by directing individuals to a chargeable telephone number.

A consumer association lodged a complaint against a company concerning video surveillance notices. Those notices directed data subjects to a chargeable 902 telephone number to exercise their rights of access and objection. The use of a chargeable telephone number was contrary to the GDPR requirement that such rights be exercisable free of charge and could discourage data subjects from exercising them. The availability of other free channels on the website did not remedy the issue. The AEPD found an infringement of Article 12(2) GDPR. As a corrective measure, it ordered the company to replace the notices within twelve months.

For more information: [AEPD decision](#) [ES]

09/14/2026

AEPD | Notification | Data Breach Caused by AI Agent

The AEPD has received the first notification of a personal data breach caused by an attack executed using an AI agent.

According to the affected organization, the attacking agent searched for vulnerabilities in generic files and performed a successful login. Once inside the system, it autonomously looked for vulnerabilities allowing it to modify personal data and access invoices. For the AEPD, the relevant point is that a third party appears to have used an AI agent to chain the different phases of the attack. This first notification is a significant signal that AI-supported attacks now affect real processing of personal data. The AEPD asks that attacks assisted or executed by AI be expressly included in the risk analyses of processing operations.

For more information: [AEPD website](#) [ES]

United Kingdom

09/30/2026

ICO | Institutional Reform | Transition to the Information Commission

On 30 September 2026, the Information Commissioner's Office (ICO) formally became the Information Commission, a new body corporate created by the Data (Use and Access) Act 2025.

The Office of the Information Commissioner, which previously operated as a "corporation sole" vesting statutory powers in a single office-holder, was abolished and replaced by the Information Commission (the ICO abbreviation will continue to be used, referring to the Information Commission's Office). All functions, staff and ongoing matters transferred automatically to the new body. The Information Commission will be governed by a board composed of a Chair, a Chief Executive Officer and non-executive members, with collective responsibility for its decisions, a structure similar to that of other UK regulators such as the Financial Conduct Authority and the Competition and Markets Authority. Seven non-executive members of the new board, announced in July 2026, assumed their roles on the same date, with Paul Arnold appointed as the first Chief Executive. One of the board's first decisions was to appoint Maggie Carver (one of the non-executive members) as Deputy Chair. She will perform the Chair's functions on an interim

basis while the UK Government continues the appointment process for the first Chair, expected to conclude in spring 2027.

For more information: [ICO website](#)

09/17/2026

ICO | Blog | Smart Glasses and Wearable Technologies

The ICO's Chief Executive highlighted the privacy implications of smart glasses and other AI-enabled wearables, calling for safeguards against covert recording while preserving beneficial uses such as assistive technology.

The ICO warns that increasingly discreet wearable devices make it harder for individuals to know when data about them is being captured, raising transparency concerns in public spaces. It urges companies to embed privacy by design, minimize unnecessary data collection, and invest in safeguards. The ICO also notes that recordings shared publicly online are unlikely to fall within the exemption for purely personal or household activities. It considers the challenges posed by wearables to extend beyond data protection law to social norms, product standards and potential future legislation, and is preparing a consultation on its AI and automated decision-making code in 2027. No device-specific guidance on smart glasses is currently expected.

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

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](http://www.gibsondunn.com).

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](http://www.gibsondunn.com/privacy).

[Preferences](#) | [Unsubscribe](#) | [Forward](#)

[View online](#)