View in browser



Privacy, Cybersecurity, and Data Innovation Update November 12, 2026

European Data Privacy Newsletter

We are pleased to provide you with the October 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

10/21/2026

Council of the EU | Legislative Process | Digital Omnibus

The Council has agreed its negotiating position on the proposal to simplify certain EU rules on data protection, privacy and cybersecurity.

Part of the Omnibus VII package, the proposal amends the GDPR, updates the cookie rules of the ePrivacy Directive and introduces a single mechanism for reporting cyber and data incidents. In its position, the Council keeps the current definition of personal data and adds a provision under which pseudonymized data is not personal data for a recipient that cannot identify the individuals concerned. It also simplifies the rules on unfounded or excessive data subject requests and on information obligations in low risk situations. It adds safeguards to the new derogation allowing sensitive data to be processed for biometric verification and AI systems and supports extending the deadline for notifying personal data breaches to 96 hours, a single EU list of high-risk processing operations and common notification templates. Cookie rules would remain in the ePrivacy Directive, with more purposes

exempt from consent, such as audience measurement and device security, while each Member State would set up a national entry point for incident reporting. Negotiations with the European Parliament will start once the Parliament adopts its own position.

For more information: Council of the EU website and Council mandate

10/12/2026

European Commission | Announcement | Political Ads Repository

The European Commission has launched the pilot version of the European Repository for online political advertisements.

The Repository is provided for by the Regulation on Political Advertising, which has fully applied since 10 October 2025. Pursuant to this Regulation, political advertising publishers providing online political advertising services must make each political advertisement they disseminate, and the information provided through the related transparency notice, available in the Repository. The latter will store transparency notices on who is behind each ad, including the sponsor, controlling entity and paying entity, and on the amounts spent. It will also cover the source and origin of funding, the dissemination period and the use of targeting or ad-delivery techniques based on personal data, including AI systems. Once fully operational, it is intended to help publishers comply with the Regulation and allow researchers and journalists to scrutinize political advertising. The pilot is available for voluntary use since 12 October 2026. Political advertising publishers will only have to make their ads and transparency notices available in the Repository from its official deployment, the date of which the Commission will announce sufficiently in advance for them to prepare.

For more information: European Commission website

10/02/2026

European Commission | Consultation | EU KIDS Act

The European Commission has opened a call for feedback on the proposed EU KIDS Act.

The Commission's aim is to collect input from children, parents, guardians, teachers and educators, as well as from the online platforms covered by the proposal. Proposed in September, the EU KIDS Act aims to strengthen the online safety of children across the Union. To that end, it provides for a gradual access to social media, strong safety-by-design rules, privacy-preserving age assurance and

effective enforcement. The Commission will summarize all responses and present them to the European Parliament and Council to feed into the legislative debate. The primary feedback period, for information intended to inform the legislative debates, closes 26 November 2026, with additional feedback collected until 3 December 2026.

For more information: European Commission website

Belgium

10/23/2026

APD | Management Plan | Priorities for 2027

The Belgian data protection authority (APD) has presented its 2027 management plan, which sets out its awareness-raising and enforcement priorities for the coming year.

Its awareness-raising actions will focus on profiling and data reuse in the banking sector, health data processed notably by health apps, and booking data in the hospitality sector. The APD also plans to issue a recommendation on technical and organizational security measures. On enforcement, the APD plans to pay particular attention to data brokers and to data processing in the video game sector. The APD also plans to modernize its internal processes, including by introducing AI in its operational services.

For more information: APD website [FR]

Denmark

10/09/2026

Datatilsynet | Decision | Right of Access

The Danish data protection authority (Datatilsynet) considered that an employer could lawfully refuse a former employee's access request in view of decisive private and public interests.

A former employee had requested access to the material his employer had relied on to dismiss him, including an exchange of private messages between him and

another former employee. The employer refused. The material was also at issue in private criminal proceedings brought by the employee. Under the Danish Data Protection Act, the right of access may be restricted where the data subject's interest must give way to decisive private or public interests. The Datatilsynet considered that protecting the persons involved in these proceedings and ensuring their proper conduct were such interests, so the employer was entitled to refuse. It took no position on whether the employer had been entitled to access the messages, an issue forming part of the pending proceedings. However, the Datatilsynet criticized the reasons given to the employee for the refusal: they were too general and did not sufficiently set out the specific circumstances and interests assessed, as required under Article 12(4) GDPR.

For more information: Datatilsynet website [DA]

France

10/29/2026

CNIL | Sanction | Cookies in Mobile App

The French data protection authority (CNIL) has fined two companies of a French retail group a total of 7 million euros for breaching the rules on cookies in the group's mobile app.

The CNIL acted on a complaint lodged by NOYB and inspected the companies' mobile app in March 2024. It found that the companies used a tracker on the mobile app without users' consent. This tracker collected browsing history to display product recommendations and train a recommendation algorithm. Requests containing a user identifier and activity data, such as products viewed, were sent via an API to a third-party domain. For the CNIL, these operations did not fall within the exemptions of Article 82 of the French Data Protection Act and therefore required prior consent. The amount of the fine reflects the companies' disregard of users' choice to refuse tracking and the large number of app users. It also reflects the CNIL's consistent enforcement line on trackers used for personalization and targeting purposes.

For more information: CNIL website and CNIL decision [FR]

10/16/2026

CNIL | Guidance | Inferring Professional Email Addresses

The CNIL has clarified the conditions under which organizations may infer professional email addresses from data available online.

This practice consists of inferring, or "guessing", an address from a person's name and their employer's email format, for example for B2B prospecting. The fact that the data is accessible online does not exempt organizations from the GDPR. The practice may rely on legitimate interest if the organization has a real interest in contacting the person and does not disproportionately affect their rights. The organization must assess whether the person could reasonably expect such use. People with no identifiable online presence or who restrict access to their contact details cannot, in principle, reasonably expect their address to be inferred. Safeguards may include strictly limiting retention and immediately excluding anyone who objects. Failing this, the organization must obtain consent or refrain from inferring addresses.

For more information: CNIL website [FR]

Germany

10/21/2026

Bundesgerichtshof | Judgment | Credit Scoring

The German Federal Court of Justice (BGH) has ruled that credit scoring must be explained where the score decisively influences a company's decision to enter into, perform or terminate a contract with a person.

A German credit reference agency calculates scores estimating the probability that individuals will meet their payment obligations and provides them to its clients, such as lenders. In four parallel cases, individuals had asked the agency to explain how their scores were calculated. In line with the CJEU's judgment (C-634/21), the BGH held that the right to meaningful information about the logic involved, under Article 15(1)(h) GDPR, only applies where the scoring amounts to an automated decision within the meaning of Article 22(1) GDPR, that is, where the company's contractual decision depends decisively on the score. While it is for the individual to establish this, the BGH significantly eased the burden of proof: where the agency has transmitted a score to a company and that company has taken an adverse contractual decision shortly afterwards, the decision is presumed to have been decisively based on the score. The BGH set aside the appeal judgments and

referred the cases back to the Higher Regional Court of Dresden, which will now have to determine whether these conditions are met.

For more information: BGH website [DE]

10/12/2026

Lower Saxony DPA and other State DPAs | Guidance | Phishing with Stolen Hotel Booking Data

Several German state data protection authorities have reminded accommodation businesses of their obligations under the GDPR in light of increasing fraudulent messages sent to hotel guests after cyberattacks.

The Mecklenburg-Western Pomerania DPA (LfDI MV) reported a significant increase in breach notifications and published an information letter for accommodation businesses on October 5, 2026. Several DPAs in Germany followed, referring to a "massive accumulation" of breach notifications and consumer complaints. The Lower Saxony DPA also recorded more breach notifications from the tourism sector in the third quarter of 2026, notably after cyberattacks on booking service providers. The Lower Saxony and LfDI MV letters stress that hotels remain responsible for their guests' data even where an external provider manages bookings. Therefore, they must notify the breach to the competent supervisory authority and inform all affected guests, not only those who have already received fraudulent messages. The letters also contain a practical checklist and refer to the EDPB Guidelines 9/2022 on personal data breach notification.

For more information: LfD Niedersachsen website, LDI NRW website and LfDI MV website [DE]

10/06/2026

BfDI | Press Conference | Priorities of the New Commissioner

Moritz Hennemann, the new Federal Commissioner for Data Protection and Freedom of Information (BfDI), has presented the priorities of his term of office at the Federal Press Conference.

His term will focus on three areas: data protection-compliant modernisation of the State, the digital sovereignty of Germany and the EU, and the early data protection assessment of major technological leaps. He intends to give early, solution-oriented advice to the bodies he supervises and also wants to work even more closely with supervisory and regulatory authorities, including for effective enforcement. He has

warned against blanket restrictions in the reform of freedom of information law. He took office on 1 October 2026, succeeding Louisa Specht-Riemenschneider.

For more information: BfDI website and opening statement [DE]

10/05/2026

Verwaltungsgericht Düsseldorf | Judgment | Proof of Consent to Email Marketing

The North Rhine-Westphalia DPA (LDI NRW) has reported that a judgment of the Düsseldorf Administrative Court (VG Düsseldorf) of 27 July 2026 upholding a reprimand it had issued against a company that could not prove the consent of a recipient of its advertising emails has become final.

A company had sent advertising emails to a complainant who denied ever having provided his email address. The company claimed that he had given his consent on its website. He kept receiving advertising emails even after the LDI NRW had intervened. As the company could not produce a confirmation email, the LDI NRW issued a reprimand (Verwarnung) under Article 58(2)(b) GDPR and the company's action against it was dismissed. According to the court's headnotes, where the controller cannot demonstrate the lawfulness of the processing in accordance with Article 7 GDPR, consent is deemed not to have been (validly) given. The mere indication of an email address, an IP address and a double opt-in IP address with time stamps is unsuitable to prove consent, since such data do not show who was acting. The court also noted that the company had not followed its own procedure of archiving confirmation emails. It concluded that no confirmation email existed.

For more information: LDI NRW website and judgment [DE]

Italy

10/05/2026

Garante | Guidelines | Tracking Pixels

The Italian data protection authority (Garante) reminded companies and platforms that they had until 29 October 2026 to comply with its guidelines on tracking pixels in emails.

Controllers had until 29 October 2026 to adapt their privacy notices, consent mechanisms and withdrawal systems in email communications. Tracking pixels are images inserted into emails that detect when a message is opened and collect information on user behavior. The Garante stressed that they can be particularly invasive, as they often operate without the recipient's full awareness. Their use falls under Article 122 of the Italian Privacy Code, which regulates the use of technologies capable of accessing information on users' devices or monitoring their online behavior, while the GDPR sets the general framework on transparency, consent, accountability and data protection by design and by default. Prior, free, specific and informed consent is therefore required, subject to specific exceptions. Users must also receive clear and transparent information and be able to withdraw their consent easily, including selectively. The Garante also drew attention to privacy by design and by default measures aimed at reducing the risk of users being identified and limiting the circulation of personal data. It added that checks on compliance are among the inspection activities planned for the second half of 2026.

For more information: Garante website [IT]

Netherlands

10/29/2026

AP | Recommendations | AI in Debt Collection

The Dutch data protection authority (AP) issued recommendations to the debt collection sector after a sample of 29 agencies showed an increasing use of algorithms and AI.

According to the AP, these tools speed up the work but create risks of incorrect decisions, discrimination and unequal treatment. Beyond chatbots and conversation reports, many agencies use AI to estimate the likelihood of successfully collecting a debt. The system relies on variables such as credit score, location and payment history, and helps staff decide which debtors to approach first. Agencies also "enrich" debtors' files with contact, bank or company details and social media activity found in registers or online. The AP three main recommendations are to (i) provide human intervention in decisions with a significant impact on debtors, (ii) map the personal data processed against privacy law, and (iii) improve the information provided to debtors by clearly explaining how algorithmic systems are used and actively informing them of their rights.

For more information: AP website [NL]

10/16/2026

AP | Investigation | Misleading Cookie Banners

The AP has opened an investigation into two organizations that keep using a misleading cookie banner on their website, despite having received an explanation and a warning.

The cookie banners of these organizations do not have a directly visible button to refuse tracking cookies. As a result, visitors are more likely to accept them. The AP states that refusing tracking cookies must be as easy as accepting them, so a directly visible refuse button must sit next to the accept button. Since 2024, the AP has been checking more often whether organizations correctly request consent for tracking cookies. In recent months, it has warned around 100 organizations, notably in the media, healthcare and insurance sectors. About 70% of organizations adjust their banner after a warning. Those that do not comply can expect an investigation and possibly a fine.

For more information: AP website [NL]

Poland

10/16/2026

UODO | Announcement | Political Advertising

The Polish data protection authority (UODO) states that the presidential veto of the national law on political advertising does not affect its powers under Regulation (EU) 2024/900.

The Polish President refused to sign the Act of 4 September 2026, which was intended to ensure the full application of the Regulation by designating the competent authorities, providing for penalties and regulating the procedures before these authorities. For the UODO, the provisions of this act were merely organizational, as its powers derive directly from the Regulation, applicable since 10 October 2025. Article 22(1) of the Regulation makes data protection authorities competent to monitor the requirements on targeting and ad-delivery techniques in online political advertising. Article 58 and Chapter VII of the GDPR apply accordingly to this supervision. The UODO may also impose fines under Article 83 GDPR. However, the Regulation contains wider obligations that remain outside the UODO's remit.

For more information: UODO website [PL]

10/05/2026

UODO | Guidance | Data Breach Notification

Following recent data breaches affecting thousands of entities, the UODO reminds controllers that not every breach must be notified to it.

Under Article 33(1) GDPR, a breach must be notified unless it is unlikely to result in a risk to individuals' rights and freedoms. The recent reported incidents mainly involved unauthorized access to contractor databases and invoicing systems. The UODO explains that controllers must carry out a thorough risk assessment in each case but that notification is usually not required where only data publicly available in the Polish business register (CEIDG) is disclosed, such as names, company names, tax numbers or business addresses. A notification is required where other information that could enable fraud, identity theft, profiling or social engineering is also exposed. In all cases, controllers must document the risk assessment and record the reasons for not notifying in their internal breach register.

For more information: UODO website [PL]

Spain

10/07/2026

AEPD | Guidance | Algorithms and Employment Environment

The Spanish data protection authority (AEPD) has published a guidance note on the use of algorithms in the employment environment.

Royal Decree 723/2026, which entered into force on 5 October 2026, requires employers to inform each worker in writing of the existence of algorithmic or automated decision-making systems. Where these systems are used to decide on working conditions, their guidelines, criteria and operating rules must also be explained. The AEPD clarifies that this new labor obligation does not displace the GDPR. When personal data are processed, employers must comply with both sets of rules at the same time. The note also presents the AEPD's warning on an AI tool, not yet deployed, designed to screen, score and prioritize candidates in recruitment and internal mobility. The AEPD recalls that risks must be assessed and a DPIA carried out before the processing where a high risk is likely. Data protection by design and by default, security measures and clear information are also required.

Finally, human intervention must be effective: the reviewer must be able to critically assess the score and depart from it.

For more information: AEPD note [ES]

10/06/2026

AEPD | Warning | AI Video Surveillance

The AEPD has issued warnings to two municipalities whose video surveillance projects include AI functionalities for the automated analysis of images.

One project includes facial detection or recognition features while the other provides for the detection of people, vehicles and the generation of metadata. The AEPD points out that data protection law does not prevent the use of these technologies. However, it requires safeguards adapted to their characteristics and risks. Data protection must therefore be built in from the earliest stages of the project. Before deployment, controllers must assess which functionalities are necessary and whether their use is proportionate. The mere technical availability of a capability to identify, search for, locate or track individuals does not in itself justify its use. A DPIA must be carried out where the processing is likely to result in a high risk. If a functionality involves biometric data used to uniquely identify a person, the reinforced regime for such data applies and specific safeguards must be put in place. Individuals must also receive clear, accessible and understandable information. These warnings are preventive, as the processing has not yet started, and do not mean that an infringement has been committed.

For more information: AEPD website [ES]

United Kingdom

10/29/2026

ICO | Statement | Age Assurance

The ICO has welcomed Ofcom's rapid assessment of highly effective age assurance at the 16-age threshold and its report on app stores.

According to the ICO, age assurance plays an important role in its shared goal with Ofcom of protecting children from harm online. However, it must be implemented in a way that keeps personal data safe. It must also allow people to exercise their information rights. The ICO is working closely with the Government and Ofcom to

ensure that data protection is taken into account as the new regulations are developed. In its assessment, Ofcom identified four methods currently capable of being highly effective at determining whether a user is 16 or over: photo ID matching, digital identity services, banking-based checks and facial age estimation. This work complements its own assessment of how age assurance providers currently comply with data protection law.

For more information: ICO website

10/14/2026

ICO | Reprimand and Enforcement Notice | Use of Unapproved Third-Party Platform

The ICO has issued a reprimand and an enforcement notice to the Metropolitan Police Service (MPS) after officers and staff shared personal data through an unapproved third-party retail crime intelligence platform.

Between March 2023 and September 2024, MPS officers and staff registered around 500 free accounts on the platform, which retailers use to share reports and CCTV footage about suspected retail crime, without the safeguards required for a new processing tool. The ICO found that the MPS had processed personal data unlawfully where sharing was not necessary for law enforcement purposes, had not put in place appropriate measures for approving third-party technologies, and had not carried out a DPIA before high-risk processing. The MPS suspended use of the platform in September 2024 and reintroduced it in January 2026 after completing a DPIA, adding contractual controls and training staff. The enforcement notice, issued on 23 September 2026, requires the force to strengthen how it assesses and approves third-party services and to report periodically to the ICO.

For more information: ICO website

10/09/2026

ICO | Guidance | Smart Data Schemes

The ICO has published guidance for Smart Data scheme designers on how data protection law applies to sharing customer data with authorized third parties.

Smart Data schemes, provided for by the Data (Use and Access) Act 2025, build on Open Banking and let customers share their data securely with authorized third parties to access new services or compare products. The guidance targets scheme designers, such as government departments, regulators and scheme operators,

which set scheme rules without necessarily processing the data. It sets out the ICO's expectations on controller, joint controller and processor roles, on lawful basis (a customer's "consent" to share data is not necessarily UK GDPR consent), and on transparency, data minimization, data subject rights, security, complaints and data protection by design and by default. The ICO will not approve individual schemes.

10/01/2026

ICO | Partnership | Cyber Resilience

The ICO has become a member of the National Cyber Resilience Centre Group's (NCRCG) National Ambassador Programme to strengthen cyber resilience across the UK.

Through this partnership, the ICO will work with the other National Ambassadors and the network of police-led Cyber Resilience Centres. Together, they will raise awareness of cyber security risks and direct SMEs to free and affordable support across the UK. Cyber security is one of the ICO's key regulatory priorities. The initiative comes as cyber threats keep evolving and organizations find it increasingly difficult to keep personal information secure. The ICO notes that many cyber incidents result from organizations failing to get the basics right and will therefore promote the support offered by regional Cyber Resilience Centres. The ICO encourages organizations to act now to strengthen their cyber security, without waiting for an incident.

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