Privacy, Cybersecurity, and Data Innovation Update July 12, 2024

European Data Privacy Newsletter

Q1 and Q2 2024

Europe

07/12/2024

European Union | Artificial Intelligence Regulation | Publication

The AI Act (Regulation 2024/1689) was published in the OJEU today. It will enter into force on 1 August, meaning the 2-year transition period for most of the Act will end on 1 August 2026.

The Act applies to AI providers, deployers, importers, distributors, and manufacturers, with exemptions for military and research uses. It classifies AI systems by risk, prohibits certain practices, and in particular imposes requirements on high-risk systems. Enforcement includes the creation of an AI Office, a scientific panel, an AI Board, and an advisory forum, with possible fines up to €35 million or 7% of global turnover for severe breaches.

For more information: Official Journal of the European Union

06/20/2024

Court of Justice of the European Union | GDPR Violation | Right to Compensation

The Court of Justice of the European Union ("CJEU") published a judgment on the right to compensation for non-material damage as a result of fear.

In the case C-590/22, the CJEU ruled that an infringement of the GDPR alone does not suffice to establish a right to compensation. The claimant must demonstrate actual damage caused by the infringement, although the damage need not be severe. The CJEU also determined that a claimant's fear of personal data disclosure to third parties — as a result of a breach of the GDPR — can constitute non-material damage if the fear and its negative consequences are duly demonstrated. Notably, the criteria for administrative fines do not apply to compensation assessments, and compensation is not meant to serve a dissuasive function. Furthermore, violations of national laws that do not specifically relate to the GDPR do not need to be considered when determining compensation amounts.

For more information: CJEU Judgment- C-590/22

06/20/2024

Court of Justice of the European Union | GDPR Violation | Right to Compensation

The Court of Justice of the European Union ("CJEU") published rulings on the right to compensation for non-material damages based on theft of personal data.

The CJEU made several important rulings regarding compensation under Article 82(1) of the GDPR. First, the court clarified that the right to compensation is intended solely to fully compensate for the damage suffered due to GDPR violations and does not serve a punitive purpose. Second, the severity or intentional nature of the violation does not need to be considered when determining the amount of compensation. Third, the court emphasized that non-material damage from a data breach is not inherently less significant than physical injury. Furthermore, minimal compensation can be awarded for minor damage as long as it fully compensates the harm. Finally, the court stated that for identity theft under the GDPR, actual misuse of stolen data must be shown, but compensation for non-material damage is not limited to cases where identity misuse is proven.

For more information: CJEU Judgment - C-182/22 and C-189/22

04/18/2024

European Data Protection Board | Strategy | Priorities for 2024-2027

On April 18, 2024, the European Data Protection Board ("EDPB") released its strategy for 2024-2027.

The EDPB aims to support supervisory authorities in enforcing the GDPR and the Law Enforcement Directive, while also facilitating their interaction with new legislation such as the EU AI Act, the Digital Services Act, and the Digital Markets Act. Specifically addressing artificial intelligence, the EDPB plans to offer guidance on data protection and GDPR implementation, focusing on high-risk areas and vulnerable groups, such as children. Regarding the EU-US Data Privacy Framework, the EDPB intends to provide public information and template complaint forms to facilitate the implementation of redress mechanisms.

For more information: EDPB Website

03/14/2024

Court of Justice of the European Union | Personal Data | Powers of the Supervisory Authority

The Court of Justice of the European Union ("CJEU") ruled that the supervisory authority of a Member State may order, of its own motion, the erasure of personal data in case of unlawful processing.

The CJEU clarified that the supervisory authority is entitled to order the erasure of data in order to ensure that the GDPR is fully enforced, even in the absence of a prior request made by the data subject to that effect. The CJEU further specified that, like other corrective measures, the power of the supervisory authority to order the erasure of data applies regardless of whether the data is collected directly from the data subject or indirectly from another source.

For more information: CJEU Judgment - C-46/23

04/11/2024

Court of Justice of the European Union | Compensation | GDPR Violation

In a ruling issued on April 11, 2024, the Court of Justice of the European Union ("CJEU") clarified the concept of non-material damage, the conditions for exemption from liability and the criteria for determining the amount of damages.

Referring to its previous case law, the CJEU ruled that the mere infringement of GDPR provisions granting rights to individuals is insufficient to establish non-material damage, unless the individual can prove actual harm, regardless of its severity. The Court emphasized that an organization cannot evade liability simply by attributing the infringement to human error within its operation. Additionally, when assessing compensation for non-material damages under GDPR, the criteria for setting administrative fines are not applicable, nor should the quantity of infringements affect

compensation calculations. The judgment asserts the need for full and effective compensation directly proportional to the actual damage suffered, adhering strictly to the compensatory rather than punitive intent of the provision.

For more information: CJEU Judgment - C-741/21

03/07/2024

Court of Justice of the European Union | Personal Data | Online Advertising

The Court of Justice of the European Union ("CJEU") rendered its judgment in the IAB Europe case and clarified the organization's status with regard to data processing operations for advertising purposes within the Transparency and Consent Framework ("TCF").

The TCF is a set of rules established by IAB Europe, consisting of guidelines and technical specifications that enable its members (website or application providers, data brokers, and advertising platforms) to lawfully process the personal data of users of a website or an application. The TCF allows, *inter alia*, the recording of users' preferences through Consent Management Platforms, by generating a signal called "TC String". First, the Court confirmed that the TC String is personal data within the meaning of the GDPR since it contains certain information that can be used to identify a user if associated with an identifier, such as an IP address. Second, the Court held that IAB Europe is a joint controller with its members when the consent preferences are recorded in a TC String. However, the Court stated that IAB Europe cannot be regarded as a controller for the subsequent data processing operations by members.

For more information: CJEU Judgment - inter alia

03/07/2024

Court of Justice of the European Union | Personal Data | Concept of Processing

The Court of Justice of the European Union ("CJEU") ruled that the oral disclosure of information on possible ongoing or completed criminal proceedings to which a natural person has been subject constitutes processing of personal data.

The CJEU reiterates that since the oral disclosure of personal data constitutes non-automated processing, the personal data subject to such processing must be contained or intended to be contained in a filing system in order for that processing to fall within the material scope of the GDPR. The CJEU states that, in the present case, information on criminal proceedings is contained in a register of persons kept by a court, i.e., a filing system. Therefore, any oral disclosure of its contents may take place only if the conditions imposed by the GDPR are satisfied.

For more information: CJEU Judgment - C-740/22

03/07/2024

Court of Justice of the European Union | Personal Data | Concept of Identifiable Person

The Court of Justice of the European Union ("CJEU") annulled a judgement issued by the General Court for misinterpreting the concept of "identifiable natural person".

The case concerns a compensation claim brought before the General Court by a scientist with regard to a press release published by the European Anti-Fraud Office. In its judgement, the General Court had held that information contained in the press release did not constitute personal data since the person concerned was not identifiable with that information alone. The CJEU referred to its previous case law and stated that for information to be considered as "personal data", it is not required that all the information enabling the identification of the data subject is in the hands of one person. In the present case, the data subject could be identified, in particular, by persons working in the same scientific field.

For more information: CJEU Judgment - C-479/22 P

02/13/2024

European Data Protection Board | Opinion | Notion of Main Establishment

The European Data Protection Board ("EDPB") adopted an Opinion on the notion of main establishment and the criteria for the application of the One-Stop-Shop mechanism following a request by the French Supervisory Authority.

The Opinion clarifies the notion of a controller's "main establishment" in the EU, in particular in cases where decisions regarding the processing are taken outside the EU.

For more information: EDPB Website

01/18/2024

European Data Protection Board | Case Digest | Data Breach

The European Data Protection Board ("EDPB") published a thematic one-stop-shop case digest on security of processing and data breaches.

The case digest analyses decisions adopted by supervisory authorities under the one-stop-shop mechanism relating to security of personal data and personal data breaches. It is intended to

provide insights on how supervisory authorities have applied the relevant GDPR provisions in different data breach scenarios, such as ransomware or accidental data disclosure.

For more information: EDPB Website

01/11/2024

European Union | Regulation | Data Act

The Regulation on harmonized rules on fair access to and use of data ("Data Act") entered into force.

The Data Act introduces, in particular, new data sharing and contractual obligations for providers of connected devices and related services, as well as cloud computing providers. The Act will become applicable 20 months from the date of entry into force, i.e., from September 12, 2025. Requirements on access to data generated by connected devices will apply to devices placed on the market after September 12, 2026.

For more information: Official Journal of the European Union

01/07/2024

European Union | Regulation | Cybersecurity

The new Cybersecurity Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union entered into force.

The regulation aims to achieve a high common level of cybersecurity within Union entities by introducing an internal risk management, governance, and control framework, and establishing an Interinstitutional Cybersecurity Board to monitor its implementation.

For more information: Official Journal of the European Union

France

06/10/2024

French Supervisory Authority | Public Consultation | Artificial Intelligence

On June 10, 2024, the French Supervisory Authority ("CNIL") opened a public consultation on its AI recommendations.

The consultation primarily focuses on the legal basis of processing for AI models' development phase, data scraping for model training, and distribution of open-source AI models. It also covers other GDPR-related issues such as informing data subjects and the management of their rights.

For more information: CNIL Website

05/22/2024

French Parliament | Regulation | SREN Act

The Securing and Regulating the Digital Space Act ("SREN Act") has been published in the Official Journal.

The SREN Act introduces a wide range of provisions in areas such as online child protection, cloud services, and Jonum (i.e., games offering monetizable digital objects). Additionally, it aims to align French law with the Digital Services Act ("DSA") and the Digital Markets Act ("DMA"). With regard to the DSA, the Arcom is designated as the "digital services coordinator". While the DGCCRF will be in charge of monitoring marketplace providers' compliance with their obligations, the French Supervisory Authority will be responsible for ensuring that platforms comply with requirements related to online advertising. Regarding the DMA, the French Competition Authority and the Ministry of the Economy will be able to investigate and cooperate with the European Commission on gatekeepers' practices. Furthermore, the SREN Act addresses the adaptation of French law to the Data Act and the Data Governance Act and grants new powers to regulatory bodies.

For more information: Official Journal [FR]

05/14/2024

French Supervisory Authority | Guidance | Traffic Data

On May 14, 2024, the French Supervisory Authority ("CNIL") issued guidance on providing public internet access, emphasizing legal obligations for retaining traffic data.

Under the French law, organizations providing public internet access must retain IP addresses to identify devices, connection details (date, time, duration), and data identifying communication recipients. In this context, the CNIL reiterated that traffic data, being personal data, should be limited to what is necessary for processing. The retention periods vary according to the concerned data (from 3 months to 5 years).

For more information : CNIL Website [FR]

04/04/2024

French Supervisory Authority | Sanction | Direct Marketing

The French Supervisory Authority ("CNIL") fined a telecommunications equipment retailer €525,000 for unlawfully processing its prospects' personal data collected from data brokers for direct marketing.

The CNIL found that the data collection forms used by data brokers were misleading and did not allow the acquisition of free and unambiguous consent to marketing texts by third parties. The French Authority pointed out that contractual obligations imposed on data brokers were not sufficient to ensure that prospects' consent was validly obtained, and the retailer should have implemented effective controls in this respect. With regard to the legal basis of marketing calls, the CNIL noted that the retailer could not validly rely on legitimate interest since the forms used by data brokers did not systematically mention the retailer in the list of data recipients.

For more information: CNIL Website

Germany

06/17/2024

Bavarian Data Protection Commissioner | Guidance | Joint Controllers

The Bavarian Data Protection Commissioner ("Bavarian DPC") published guidance on joint controllers.

The Bavarian DPC's new guidance aims at eliminating uncertainties and inhibitions in connection with joint controllership (Article 26 GDPR), which is always relevant when two or more controllers jointly determine the purposes and means of the processing of personal data. As the Bavarian DPC is the competent authority for public administration, the recommendations for action are primarily directed at stakeholders of the public sector and the examples in the guidelines are selected accordingly.

For more information: Bavarian DPC Website [DE]

05/14/2024

German Parliament | Regulation | Digital Services Act

The German Parliament aligned German law with the EU Digital Services Act ("DSA").

The German Digital Services Act (*Digitale-Dienste-Gesetz*, "DDG") accompanies the DSA and aligns German law with it at the national level. With the DDG entered into force on May 14, 2024, the German Telemedia Act (*Telemediengesetz*) lost its effect and is now replaced by the DSA and the DDG. In addition, the Telecommunications Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutz-Gesetz*) has been renamed the Telecommunications Digital Services Data Protection Act (*Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz*).

For more information: German Federal Government Website [DE]

05/06/2024

German Supervisory Authorities | Guidance | Artificial Intelligence

The German Data Protection Conference ("DSK") released guidance on artificial intelligence and data protection.

The new guidance focuses on the use of generative AI models by organizations and recalls their obligations in terms of data privacy, such as carrying out a Data Protection Impact Assessment, identifying a proper legal basis, and providing information to data subjects.

For more information: DSK Website [DE]

Italy

06/26/2024

Italian Supervisory Authority | Enforcement | Prospection

The Italian Supervisory Authority ("Garante") published its decision of June 6, issuing a fine of €6.4 million to an energy company for illicit marketing calls.

The Garante found that marketing calls had been made without data subjects' consent or despite the registration of their numbers on the Do Not Call List. In addition to the fine, the Garante ordered the company to cease further processing of the complainants' personal data and to send them the Garante's decision.

For more information: Garante Website

05/20/2024

Italian Supervisory Authority | Investigation | Web scraping

On May 20, 2024, the Italian Supervisory Authority ("Garante") issued guidelines on web scraping by public and private entities acting as data controllers.

The guidelines address the indiscriminate collection of online data by third parties, particularly for training generative AI models. The Garante recommends several measures to prevent or hinder web scraping, namely, creating reserved areas that require registration to access data, including anti-scraping clauses in websites' terms of use, monitoring web traffic to detect abnormal data flows, and implementing technological solutions to block unwanted scraping. The Garante noted that current investigations into the legality of web scraping based on legitimate interests are still pending, and the guidelines are part of interim measures.

For more information: Garante Website [IT]

03/07/2024

Italian Supervisory Authority | Sanction | Personal Data Breach

The Italian Supervisory Authority ("Garante") imposed a €2.8 million fine on a bank following a cyber-attack that occurred in 2018, and a €800,000 fine on the bank's service provider in charge of carrying out security tests.

The Garante stated that the cyber-attack had affected the data of approximately 778,000 former and current customers and resulted notably in the identification of over 6,800 customers' PINs (personal identification number) to the mobile banking portal. The Garante concluded that the bank had not adopted necessary security measures to effectively counter cyber-attacks and had not required its customers to create stronger PINs. The Garante also found that the bank's service provider had failed to notify the data breach to the bank within the required deadline and had engaged a sub-processor for the performance of security tests without prior consent of the bank.

For further information: Garante Website [IT]

Norway

07/01/2024

Oslo District Court | Judgement | Dating service

The Oslo District Court has confirmed a fine of NOK 65 million (about €5.7 million) imposed by the Norwegian Data Protection Authority on a dating service.

The fine was originally imposed by the Norwegian data protection authority (“Datatilsynet”) in 2020 because the dating service passed on too much information to advertising companies. In particular, GPS-data was affected. According to Datatilsynet, the use of the app itself involves particularly sensitive data, which is why the company has violated Article 9 GDPR. The case was triggered by a complaint from the Norwegian Consumer Council (“Forbrukerradet”). Datatilsynet's opinion has now been confirmed by the Oslo district court.

For more information: Oslo Tingrett Website [NOR]

Netherlands

06/04/2024

Dutch Supervisory Authority | Guidance | Cookies

The Dutch Supervisory Authority (“AP”) has published guidelines on cookie consent.

In its guidelines, the AP gives guidance on how to design cookie banners to ensure that they comply with consent requirements and provides concrete examples.

For more information: AP Website [NL]

05/01/2024

Dutch Supervisory Authority | Guidelines | Data Scraping

On May 1, 2024, the Dutch Supervisory Authority (“AP”) released guidelines regarding data scraping practices by private individuals and organizations.

The guidelines emphasize GDPR compliance in data scraping endeavors, mandating adherence to the principles of legality, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. The AP also clarifies situations where the GDPR does not apply,

such as scraping for personal use or targeted scrapping (e.g., an organization scrapes a news media website to get news related to its business).

For more information: AP Website [NL]

Spain

05/14/2024

Spanish Supervisory Authority | Guide | Cookie

On May 14, 2024, the Spanish Supervisory Authority ("AEPD") released an updated guide on cookie use to align it with Opinion 08/2024 on valid consent in "consent or pay" models by the European Data Protection Board ("EDPB").

The AEPD incorporates the EDPB's guidelines into its own guide, and notes that the EDPB plans to issue a comprehensive guide on consent validity in "consent or pay" models by early 2025.

For more information: AEPD Website [ES]

04/12/2024

Spanish Supervisory Authority | Sanction | GDPR violations

On April 12, 2024, the Spanish Supervisory Authority ("AEPD") fined a financial services company €2 million (later reduced to €1.2 million) for GDPR violations following a complaint.

As part of a verification process, the financial services company requested personal and economic data from the complainant via a form requiring consent for such data collection, without giving an option to decline. When asked for further explanation, the financial services company stated that the complainant's bank account would be blocked if consent was not provided. The AEPD found this violated GDPR Article 6(1), as the consent was not valid and there was no legal requirement for the data verification method used by the financial services company.

For more information: AEPD Website [ES]

United Kingdom

06/07/2024

UK High Court | Judgment | Data Subject Rights

On June 7, 2024, the High Court ruled in Harrison v Cameron & Another that under the UK GDPR, data subjects have the right to know the specific identities of their personal data recipients, not just the categories.

The High Court ruled that data subjects are entitled to know the specific identities of recipients who have access to their personal data. It is within the data subject's discretion to request either detailed identities or merely the categories of these recipients.

For more information: UK High Court Judgment

05/13/2024

British Supervisory Authority | Consultation | Generative AI

On May 13, 2024, the UK Data Protection Authority ("ICO") launched the fourth chapter of its consultation series on generative artificial intelligence (AI), focusing on data subject rights in relation to the training and fine-tuning of generative AI models.

The consultation highlighted several rights that individuals have under the UK GDPR, including: the right to access, the right to rectification, the right to erasure and the right not to be subjected to automated decision-making. These rights apply to personal data in various contexts, including training data, fine-tuning data, outputs of the generative AI model, and user queries. The consultation emphasized that organizations must have processes in place to enable individuals to exercise these rights throughout the AI lifecycle. The consultation outlines several obligations for organizations developing or deploying generative AI models, namely: inform individuals if their data is being processed, provide clear, accessible information about data usage and individuals' rights, justify any exemptions used and safeguard individuals' rights and freedoms, and apply privacy-enhancing technologies and techniques to protect data. The consultation also invites feedback on the effectiveness of measures to prevent unauthorized data retention and usage. Additionally, it seeks evidence on how organizations can fulfill their legal obligations while supporting innovation in generative AI.

For more information: ICO Website

05/10/2024

British Supervisory Authority | Guidance | Cyber Security Incidents

The British Supervisory Authority ("ICO") published a report on cyber security incidents.

The report focuses on five main causes of cybersecurity incidents, including phishing, brute force attacks, and denial of service. In particular, it provides case studies based on previous data breach reports received by the ICO and gives practical recommendations to reduce the risk of cyber-attacks.

For more information: ICO Website

04/03/2024

British Supervisory Authority | Strategy | Protection of Children's Privacy Online

On April 3, 2024, the British Supervisory Authority ("ICO") released its 2024-2025 Children's code strategy for protecting children's privacy online.

Key focuses include defaulting profiles to private settings, restricting profiling for ads, monitoring content feeds, and obtaining parental consent for children under 13. The ICO plans audits on educational technology, engagement with stakeholders, and international collaboration to regulate the internet effectively.

For more information: ICO Website

This newsletter has been prepared by the European Privacy team of Gibson Dunn. For further information, you may contact us by email:

Ahmed Baladi – Partner, Co-Chair, PCCP Practice, Paris (abaladi@gibsondunn.com)
Joel Harrison, – Partner, Co-Chair, PCDI Practice, London (jharrison@gibsondunn.com)
Vera Lukic – Partner, Paris (vlukic@gibsondunn.com)
Lore Leitner – Partner, London (lleitner@gibsondunn.com)

Kai Gesing – Partner, Munich (kgesing@gibsondunn.com)
Clémence Pugnet – Associate, Paris (cpugnet@gibsondunn.com)
Thomas Baculard – Associate, Paris (tbaculard@gibsondunn.com)
Hermine Hubert – Associate, Paris (hhubert@gibsondunn.com)
Billur Cinar – Associate, Paris (bcinar@gibsondunn.com)
Christoph Jacob – Associate, Munich (cjacob@gibsondunn.com)
Yannick Oberacker – Associate, Munich (yoberacker@gibsondunn.com)
Sarah Villani – Associate, London (svillani@gibsondunn.com)
Miles Lynn – Associate, London (mlynn@gibsondunn.com)