GIBSON DUNN

Gibson Dunn | Europe | Data Protection – Q4 2023

Client Alert | January 22, 2024

European Data Privacy Newsletter **Europe**

12/14/2023

Court of Justice of the European Union | Decision | Misuse of personal data

The Court of Justice of the European Union ruled that the fear of a possible misuse of personal data is capable, in itself, of constituting non-material damage.

In this case, the Bulgarian Supreme Administrative Court requested clarification of the conditions for awarding compensation for non-material damage relied on by a data subject whose personal data, held by a public agency, were published on the internet following an attack from cybercriminals. The Court emphasized that the mere occurrence of unauthorized disclosure or access to personal data does not automatically imply that the protective measures implemented by the controller were not appropriate, they must be assessed in a concrete manner. For more information: CJEU Website

12/07/2023

Court of Justice of the European Union | Decision | Automated Individual Decision

The Court of Justice of the European Union issued a significant ruling in cases involving a private credit information agency declaring that "scoring" qualifies as "automated individual decision-making" and is, in principle, prohibited by Article 22 of the GDPR.

While 'scoring' is permitted only under certain conditions, the prolonged retention of information relating to the granting of a discharge from remaining debts is contrary to the GDPR. The court emphasized the primacy of data subjects' rights and interests, asserting their right to prompt deletion when their personal data have been unlawfully processed, i.e. beyond the retention period. For more information: CJEU Website

12/05/2023

Court of Justice of the European Union | Decision | Calculation of Fines

The Court of Justice of the European Union disclosed two rulings in which it shared an interpretation of the GDPR concerning the assessment and computation of penalties for breaches.

The CJEU clarifies the conditions under which national supervisory authorities may impose an administrative fine on one or more controllers for an infringement of the GDPR. In particular, it holds that the imposition of such a fine requires that a wrongful conduct; in other words, that the infringement has been committed intentionally or negligently. Moreover, where the addressee of the fine forms part of a group of companies, the

Related People

Ahmed Baladi

Vera Lukic

Kai Gesing

Joel Harrison

Alison Beal

Clémence Pugnet

Thomas Baculard

Hermine Hubert

Christoph Jacob

Yannick Oberacker

Sarah Villani

calculation of that fine must be based on the turnover of the entire group. For more information: CJEU Website

11/27/2023

European Commission | Data Act

The European Regulation 2023/2854, often referred to as the "Data Act", has been adopted on 27 November 2023 and entered into force on 11 January 2024.

For more information: Council of the European Union Website

11/16/2023

European Court of Justice | Decision | Indirect exercise of rights

On November 16, 2023, the European Court of Justice ruled that supervisory authority's decisions in the context of the indirect exercise of the data subject's rights are legally binding.

As a result, an appeal to the decision is possible, and the authority must provide sufficient information to the data subject to allow him/her to decide whether or not to appeal. For more information: ECJ Decision

11/16/2023

European Data Protection Board | Guidelines | Tracking technologies

The European Data Protection Board published its guidelines on the application of article 5(3) of the e-Privacy Directive on new tracking technologies.

The guidelines aims to clarify how the e-Privacy Directive applies to innovative technologies. The EDPB is open to comments until January 18, 2024. For more information: EDPB Guidelines

10/28/2023

European Commission and Japan | Agreement | Cross Border Data flows

On October 28, 2023, the European Commission has reached an agreement with Japan concerning cross-border data flows.

This agreement aims to facilitate efficient data handling between both parties, eliminating burdensome administrative and storage requirements. Notably, the agreement removes the requirement for companies to physically store their data locally. Once ratified, the provisions of this agreement will be incorporated into the EU-Japan Economic Partnership Agreement. For more information: European Commission Website

10/26/2023

Confederation of European Data Protection Organizations | Paper | Generative AI

The Confederation of European Data Protection Organizations released a paper addressing the data protection implications of Generative AI.

Key issues covered include data-sharing risks, accuracy of personal data, conducting DPIAs on generative AI tools, implementing data protection by design, selecting a lawful basis for training generative AI systems, optimizing organizational structures, applying

privacy-enhancing techniques and handling data subject rights within this technological context. For more information: CEDPO Website

10/26/2023

Court of Justice of the European Union | Decision | CJEU rules on Art. 15 GDPR (right to access)

The CJEU has clarified the rights of data subjects. The court ruled that the controller may only charge a fee for providing a copy under Art. 15 (3) GDPR where the data subject has already obtained a free copy before.

Furthermore, the data subject must receive a full copy of his/her personal data, where the provision of such a copy is essential in order to enable the data subject to verify how accurate and exhaustive those data are, as well as to ensure they are intelligible. For more information: CJEU Website

10/17/2023

European Data Protection Board | Announcement | EDPB to launch coordinated enforcement action regarding Art. 15 GDPR

The EDPB selected the topic for its third coordinated enforcement action and announced that it will be launched in 2024. The action will concern the implementation of the right of access by controllers.

For more information: EDPB Website

10/12/2023

Court of Justice of the European Union | Press Release | Data Privacy Framework

The Court of Justice of the European Union ("CJEU") dismissed a French citizen's request to suspend the execution of the EU-US Data Privacy Framework's adequacy decision.

The CJEU considered that the French citizen failed to demonstrate the necessary prerequisites for such request, as he was unable to prove that he would experience significant harm if the execution of the adequacy decision was not suspended. For more information: CJEU Website

10/05/2023

European Commission | Press Release | Contractual Clauses For AI

The Commission announced the finalization of the EU model contractual AI clauses to use in procurements of AI.

The clauses are developed for pilot use in the procurement of AI with the aim to establish responsibilities for trustworthy, transparent, and accountable development of AI technologies between the supplier and the public organization. The EU model contractual AI clauses contain provisions specific to AI systems and on matters covered by the proposed AI Act, thus excluding other obligations or requirements that may arise under relevant applicable legislation such as the GDPR. For more information: European Commission Website

09/28/2023

European Data Protection Supervisor | Blog | Data Protection & Cybersecurity

The European Data Protection Supervisor published a blog post on the interplay between data protection and cybersecurity.

The post highlights the need to take into account data protection into cybersecurity strategies, advocating collaboration between data protection officers and IT security departments. Additionally, it discusses the dual role of artificial intelligence in cybersecurity, noting its potential to enhance current cybersecurity solutions and how it also allows, for instance, the production of (fake) pictures, videos, photos, texts, and more, which cybercriminals can exploit to steal someone's identity as part of social engineering attacks. For more information: EDPS Website

09/25/2023

European Commission | Data Governance Act

The European Regulation 2022/868, often referred to as the "Data Governance Act", entered into force on 24 September 2023.

As a reminder, the regulation seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data, notably with public actors. For more information: European Commission Website

Denmark

12/07/2023

Danish Supervisory Authority | Guide | Access Rights

The Danish Supervisory Authority released guidance on access rights management, emphasizing that it is a collective responsibility within organizations.

The guide highlights that all employees, regardless of their IT security role, share the responsibility of being aware of and respecting their access rights. For further information: Datatilsynet Website [DA]

11/28/2023

Danish Supervisory Authority | Measures | Data Security

The Danish Supervisory Authority released a catalog outlining technical and organizational measures essential for ensuring security in compliance with Articles 5 and 32 of the GDPR.

The catalog suggests technical measures such as automatic encryption, multi-factor authentication, automatic access control, logging of users' personal data use, and physical access control. On the organizational front, recommendations include measures such as minimizing privileged access rights, implementing role-based access rights, documenting data access authorizations, and establishing withdrawal procedures. For further information: Datatilsynet Website [DA]

09/28/2023

Danish Supervisory Authority | Sanction | GDPR Violations

The Danish Supervisory Authority issued a DKK 1 million (approx. €134,000) fine against a hotel group for failure to delete personal data.

For more information: Datatilsynet Website [DK]

Finland

11/08/2023

Finnish Supervisory Authority | Guidance | Security Breach Notification

The Finnish Supervisory Authority published guidance on filing a data breach notification.

The guidance concerns risk assessment which should take into account consequences of the data breach from the point of view of the data subject, communication to the data subject, and completion of the notification to the supervisory authority and compliance with deadlines. For further information: Ombudsman Website [FI]

France

12/12/2023

French Competition Authority | Joint Declaration | Cooperation in data protection and competition

The French Competition Authority and the French Supervisory Authority signed a joint declaration to enhance cooperation in the areas of data protection and competition.

For more information: CNIL Website [FR]

11/24/2023

French Supervisory Authority | Recommendation | API Data Sharing

The French Supervisory Authority issued a recommendation regarding the use of application programming interfaces ("APIs") for data sharing.

The recommendation outlines three specific roles involved in the usage of APIs: the data holder, the API manager, and the data re-user. The recommendation also highlights the importance of evaluating the risks associated with APIs, considering factors like the type of database access, the security levels of authentication methods, and the categories of data involved, including sensitive data. For more information: CNIL Website [FR]

11/15/2023

French Supervisory Authority | Referential | Health Data conservation duration

The French Supervisory Authority published a referential and guidance note on retention period for health data.

For more information : CNIL Website [FR]

11/07/2023

French Supervisory Authority | Sanction | Simplified Procedure

The French Supervisory Authority ("CNIL") issued ten new decisions under its new simplified sanction procedure, introduced in 2022.

Private and public-sector players were fined a total amount of €97,000 for various violations, including failure to respond to CNIL requests, non-compliance with the principle

of data minimization (geolocation and continuous video surveillance of employee), lack of information on the processing carried out and its purposes, and failure to respect individuals' rights (in particular to respond to a request for objection). For more information: CNIL Website

10/13/2023

French National Assembly | Clarifying Bill | GDPR Scope

The French National Assembly adopted an amendment to complete the French Data Protection Law in order to clarify the scope of the GDPR and ensure that certain practices are covered by French and European obligations in terms of personal data protection.

The French Supervisory Authority identified a legal gap in the data protection legislation which allows the trading of personal data by entities not established in the EU without the knowledge of individuals. The amendment seeks to supplement French law, ensuring that the GDPR applies effectively. For more information: French National Assembly Website [FR]

10/11/2023

French Supervisory Authority | Publication | Databases Trainings For AI

The French Supervisory Authority opened to public consultation its first set of guidelines on use of artificial intelligence (AI), regarding the development of learning databases for AI systems.

For more information: CNIL Website [FR]

09/28/2023

French Supervisory Authority | Sanction | GDPR Violations

The French Supervisory Authority ("CNIL") issued a €200,000 fine against an air freight company.

During the investigation, the CNIL observed some infringements regarding, in particular, an excessive data collection, a non-compliance with the ban on processing sensitive data and data relating to offences and a lack of cooperation with the CNIL services. For more information: CNIL Website

Germany

11/29/2023

German Supervisory Authority | Opinion | EU AI ACT

The German Supervisory released its stance on the EU AI Act, emphasizing the need for a comprehensive allocation of responsibilities throughout the entire artificial intelligence value chain.

The Authority asserted that the EU AI Act should clearly outline the requirements for all parties involved, including manufacturers and providers of basic AI models. Critically, it argued against a unilateral transfer of legal responsibility to the later stages of the value chain, deeming such a shift as economically unsound and detrimental to data protection. The Authority contended that a balanced distribution of responsibilities is essential to safeguard the fundamental rights of individuals whose data undergoes processing by AI systems. For more information: DSK Website [DE]

11/02/2023

Hamburg Commissioner for Data Protection and Freedom of Information| Press Release | Behavioral Advertising

The Hamburg Commissioner for Data Protection and Freedom of Information ("HmbBfDI") issued a press release addressing a social media platform's new business model in light of the European Data Protection Board's ("EDPB") binding decision on behavioral advertising.

Following the EDPB's binding decision, the social media has provided a new option where users can choose between a free version that still includes behavioral advertising, and a paid version without this type of marketing. Referring to the Resolution of the Data Protection Conference ("DSK") on subscription models, the Hamburg Commissioner for Data Protection and Freedom of Information noted that the social media platform's payment model will have to fulfill requirements like granularity in consent, transparency, and the avoidance of misleading design tools. The German Supervisory Authority expressed various problems and are now expecting a legal assessment by the lead authority in Ireland. For more information: HmbBfDI Website [DE]

10/05/2023

German Competition Authority | Press Release | Competition

The German Competition Authority ("Bundeskartellamt") obtained commitments from an American technology services company to grant users better control of their data.

The Bundeskartellamt conducted a proceeding, based on the new instrument under competition law which allows it to intervene when competition is threatened by large digital companies. In the future, the company will have to provide its users with the possibility to give free, specific, informed and unambiguous consent to the processing of their data across services. For this purpose, the company has to offer corresponding choice options for the combination of data. The choice options must be designed so as not to guide users manipulatively towards cross-service data processing to avoid "dark patterns". Such an obligation will already result from the Digital Markets Act ("DMA") for certain company services which have recently been designated by the European Commission and, thus are not covered by the commitments. For more information: Bundeskartellamt Website

09/26/2023

German Federal Court of Justice | Decision | submits questions to CJEU regarding injunctive relief under the GDPR as well as regarding Art. 82 GDPR

The German Federal Court of Justice ("Bundesgerichtshof") asked the CJEU under Art. 267 TFEU to provide a preliminary ruling as to whether Art. 17 (right to erasure) or Art. 18 (right to restriction of processing) of the GDPR also provide for a data subject's right to request from a controller to refrain from any future illegitimate processing of personal data (injunctive relief).

Furthermore, the court asked the CJEU to clarify whether mere negative feelings such as anger, resentment, dissatisfaction, worry and fear, which, in the German court's view, may be "part of the general risk of life and everyday experience" could constitute an immaterial damage within the meaning of Art. 82 GDPR. For more information: Bundesgerichtshof Website [DE]

09/19/2023

Hamburg Commissioner for Data Protection and Freedom of Information| Press Release | Data Breach Notification

The Hamburg Commissioner for Data Protection and Freedom of Information ("HmbBfDI") published guidance on handling data breach notifications.

The guidance concerns, for instance, the cases that should be notified, the deadline that applies, and the form to use to notify the German Supervisory Authority. For more information: HmbBfDI Website [DE]

09/04/2023

Supervisory Authorities | Information Note | Data Protection Framework

The German Data Protection Conference ("DSK") published an information note to explain the background and content of the EU-U.S. Data Protection Framework.

The note is aimed at both data controllers and processors in Germany who transfer personal data to the U.S. and data subjects. In particular, the note highlights the scope and application of the new framework, the use of alternative instruments for transfers to the U.S., and the scope and enforcement of data subjects' rights vis-à-vis entities in the U.S. For more information: DSK Announcement [DE]

Ireland

09/28/2023

Irish Council for Civil Liberties | Statement | Irish Data Protection Commission

The Irish Council for Civil Liberties urged the Government to guarantee no appearance of conflict of interest in the selection of new leaders of the Irish Supervisory Authority.

For more information: ICCL Website

09/11/2023

Irish Supervisory Authority |Press Release | Unlawful Marketing

The Irish Supervisory Authority welcomed the outcome of the prosecution proceedings that were taken against several companies in Ireland for sending unsolicited marketing communications without obtaining consent. For more information: Irish Supervisory Authority Website

Italy

12/12/2023

Italian Supervisory Authority | Guidelines | Password Storage

The Italian national security agency and the Italian Supervisory Authority jointly released guidelines addressing the technical measures to be adopted for password storage.

The primary goal of the guidelines is to offer recommendations for implementing the most secure technical functions for password storage, with a focus on preventing unauthorized access by cybercriminals. The guidelines outline various techniques and minimum parameters, emphasizing the improvement of password hashing techniques and the utilization of diverse algorithms as key measures to enhance password security. The overarching aim is to bolster the protection of sensitive data and mitigate the risk of

unauthorized access. For more information: Garante Website [IT]

11/22/2023

Italian Supervisory Authority | Investigation | Web scraping

The Italian Supervisory Authority announced the commencement of an investigation into public and private websites.

The aim is to assess the implementation of adequate security measures to prevent the web scraping of personal data for the training of artificial intelligence algorithms by third parties. The investigation targets all entities, acting as controllers, based in Italy or providing services in Italy, that publicly expose personal data online. For more information: Garante Website [IT]

10/23/2023

Italian Supervisory Authority | Sanction | Inaccurate Personal Data

The Italian Supervisory Authority imposed a €10 million fine on an energy company for the activation of unsolicited contracts with inaccurate and outdated data.

The Authority also ordered corrective actions, such as implementing a contract accuracy verification system, alert systems to identify improper data acquisition, and enhancing audit procedures against sales agencies. For further information: Garante Website [IT]

Norway

09/29/2023

Norwegian Privacy Appeals Board | Decision | Sensitive Data

The Norwegian Privacy Appeals Board confirmed the decision of the Norwegian Supervisory Authority from December 2021 to issue a NOK 65 million (approx. €5,5 million) fine against a dating application.

The Authority found that the dating application disclosed its users' personal data such as GPS location, IP address, mobile phone's advertising ID, age and gender - in addition to the fact that they were using the dating application - to several third parties for behavioral marketing purposes, without a proper legal basis.

Spain

11/23/2023

Spanish Supervisory Authority | Guide | Biometric Data

The Spanish Supervisory Authority issued a guide on the use of biometric data for presence and access control, outlining criteria to ensure compliance with the GDPR and other regulations.

For more information: AEPD Website [ES]

11/02/2023

Spanish Supervisory Authority | Blog Post | Synthetic Data

The Spanish Supervisory Authority ("AEPD") provided guidance on the use and generation of synthetic data.

According to the AEPD, creation of synthetic data from real personal data is itself a processing governed by the GDPR. Therefore, it is necessary to consider the provisions of the GDPR and in particular the principle of accountability, and the assessment of a possible risk of re-identification from the created synthetic data set. For more information: AEPD Website

10/20/2023

Spanish Supervisory Authority | Sanction | Cyber Security

The Spanish Supervisory Authority issued a €1 million fine (reduced to €800,000) against a Spanish banking company for insufficiently protecting the personal data of customers.

A customer had reported that its credit card had been stolen, and the bank had not properly taken the information into account, leading to identity theft where hackers took out loans and transferred money in the complainant's name. For more information: AEPD Website [ES]

10/05/2023

Spanish Supervisory Authority | Tool | Encryption

The Spanish Supervisory Authority ("AEPD") released a tool called "ValidaCrypto", designed to evaluate encryption systems.

ValidaCripto transfers the methodology of the AEPD's previously released guidelines on cryptographic systems, to an intuitive web tool that helps to visually evaluate encryption systems' compliance with data protection requirements. For more information: AEPD Website

09/28/2023

Spanish Supervisory Authority | Blog | Privacy Enhancing Technologies

The Spanish Supervisory Authority published guidance on Privacy Enhancing Technologies.

The Blog emphasizes that the Privacy Enhancing Technologies or PETs allow to implement privacy principles, but the same tools are useful to implement the governance policies that guarantee the trust and data sovereignty in a Data Space. Therefore, PETs should be "dual-use" technologies to be efficient and effective, integrated in the core of the Data Spaces, fulfilling different purposes in the data-access sharing economy. For more information: AEPD Website

United Kingdom

12/15/2023

UK Supervisory Authority | Guidance | Transfer Risk Assessment

The UK Supervisory Authority released guidance on transfer risk assessment for entities transferring personal information to the US using Article 46 of the UK GDPR.

The guidance aims to support organizations engaged in restricted transfers of personal data to the US, employing mechanisms outlined in Article 46 of the UK GDPR. Following the Schrems II case in 2020, the guidance highlights the necessity of conducting a Transfer Risk Assessment before transferring personal data from the UK, emphasizing the

importance of Department for Science, Innovation and Technology's analysis to streamline the process. The Department of Science, Innovation and Technology analysis evaluates US laws concerning access and usage of personal information for national security and law enforcement purposes. For more information: ICO Website

12/12/2023

UK Supervisory Authority | Draft guidance | Employment practices and data protection

The UK Supervisory Authority released two draft guidance documents on data protection compliance in the areas of "keeping employment records" and "recruitment and selection".

The guidance for keeping employment records is directed at employers, outlining their obligations under the UK GDPR and the Data Protection Act 2018 concerning the collection and maintenance of worker records. It emphasizes the need for a balance between the necessity of employment records for organizational operations and the privacy rights of workers. The second draft guidance is tailored for employers and entities involved in recruitment processes, including agencies and consultancies. It addresses the intricacies of managing diverse personal data, including sensitive data, during recruitment, with a focus on protecting candidates' data protection rights. These guidance documents are open for consultation from relevant stakeholders (including employers, professional associations, those representing the interests of staff, recruitment agencies, employment dispute resolution bodies, workers, volunteers and employees, and suppliers of employment technology solutions) until 5 March 2024. For more information: ICO Website

11/09/2023

Office of Communications | Statement | Online Safety Act

On September 11, 2023, the Office of Communications ("Ofcom") announced its new role as the regulator for online safety, following the enactment of the Online Safety Act on October 26, 2023.

Ofcom's role is to make online services safer for the people who use them, by ensuring regulated services take appropriate steps to protect their users. Ofcom will set out codes of practice and guidance for companies falling under the scope of the Online Safety Act. It will have powers to take enforcement action, including issuing fines to services if they fail to comply with their duties. However, Ofcom will not responsible for removing online content, and won't require companies to remove content, or particular accounts. It should be noted that Ofcom's powers are not limited to service providers based in the UK. For more information: Ofcom Website

10/25/2023

Department of Science, Innovation and Technology | Publication | Data Transfers

The Department of Science, Innovation and Technology ("DSIT") released an executive summary and initial conclusions from the first phase of an evaluation into the implementation of the International Data Transfer Agreement ("IDTA").

This evaluation started at the beginning of the implementation period of the UK's new standard data protection clauses, the IDTA and Addendum to the European Commission's Standard Contractual Clauses for international transfers, which replace the previous EU SCCs for international transfers. The evaluation was meant to assess how businesses experienced the transition to the new clauses. A further phase of this research is planned following the end of the transitional period. DSIT will work with the ICO to reflect on the findings of the research. For more information: UK Government Website

GIBSON DUNN

10/12/2023

UK-US Data Bridge | Entry into Force | Adequate Protection

On October, 12, 2023, the Data Protection Regulations 2023 for the UK Extension to the EU-US Data Privacy Framework (UK-US Data Bridge) entered into effect.

This UK extension to the EU-US Data Privacy Framework allows businesses to transfer personal data to US certified entities listed in the EU-US Data Privacy Framework without additional safeguards. However, UK organizations must update privacy policies and document data transfer methods to comply with this new framework. For more information: The Data Protection (Adequacy) (United States of America) Regulations 2023

09/20/2023

UK Supervisory Authority | Sanction | Unlawful Marketing practices

The UK Supervisory Authority announced that it issued a fine against five companies totaling £590,000 (approx. €670,000) for unwanted marketing calls which targeted the elderly and people with vulnerabilities.

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)
- Vera Lukic – Partner, Paris (vlukic@gibsondunn.com)
- Kai Gesing – Partner, Munich (kgesing@gibsondunn.com)
- Joel Harrison – Partner, London (jharrison@gibsondunn.com)
- Alison Beal – Partner, London (abeal@gibsondunn.com)
- Clémence Pugnet – Associate, Paris (cpugnet@gibsondunn.com)
- Thomas Baculard – Associate, Paris (tbaculard@gibsondunn.com)
- Roxane Chrétien – Associate, Paris (rchretien@gibsondunn.com)
- Hermine Hubert – Associate, Paris (hhubert@gibsondunn.com)
- Christoph Jacob – Associate, Munich (cjacob@gibsondunn.com)
- Yannick Oberacker – Associate, Munich (yoberacker@gibsondunn.com)
- Sarah Villani – Associate, London (svillani@gibsondunn.com)

GIBSON DUNN

Related Capabilities

Privacy, Cybersecurity, and Data Innovation