

## GIBSON DUNN | EUROPE | DATA PROTECTION – Q4 2022

To Our Clients and Friends:

**Personal Data | Cybersecurity | Data Innovation**

**Europe**

12/27/2022 – [European Union | Regulation | NIS2 Directive](#)

**The NIS2 Directive was published in the EU’s Official Journal and shall enter into force on 16 January 2023. Member States shall adopt and publish the measures necessary to comply with this Directive by 17 October 2024.**

The Directive applies to essential and important entities operating in a defined list of sectors, outlined in the Annexes I and II of the Directive: for instance, digital infrastructures (e.g., cloud computing service providers, data center service providers, providers of public electronic communications networks or services) and digital providers (e.g., providers of online marketplaces, providers of social networking services platforms).

The Directive will set the baseline for cybersecurity risk management measures. In addition, the Directive aims to set the baseline for reporting obligations. In particular, if an incident has a significant impact on the provision of services covered by the Directive, an authority must be notified without undue delay.

For further information: [NIS2 Directive](#)

---

12/27/2022 – [European Union | Regulation | DORA](#)

**The Digital Operational Resilience Act (DORA), which focuses on preventing and mitigating cyber threats, was published in the EU’s Official Journal and shall enter into force on 16 January 2023. It will apply from 17 January 2025.**

DORA will apply to financial entities (including credit and payment institutions, electronic money institutions, crypto-asset service providers), as well as information and communication technology (ICT) third-party service providers. In particular, financial entities’ management body will be responsible to define, approve and oversee the management of ICT risks. Financial entities will also have requirements on reporting major ICT-related incidents to the competent authorities. In addition,

DORA contains requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities.

For further information: [DORA Regulation](#)

---

12/27/2022 – [European Commission](#) | [Data Transfers](#) | [SCCs](#)

**Since 27 December 2022, controllers and processors are no longer able to rely on the old standard contractual clauses (SCCs) but are required to use the modernized set of SCCs.**

On 4 June 2021, the Commission issued modernized standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). The transition period to replace data transfer agreements that were based on the old SCCs and entered into before 27 September 2021 expired on 27 December 2022.

For further information: [EU Commission Website](#)

---

12/15/2022 – [Court of Justice of the European Union](#) | [Opinions](#) | [Right of Access](#)

**The Advocate Generals (“AG”) of the Court of Justice of the European Union issued two separate opinions in cases C-487/21 and C-579/21 on the right of access pursuant to Article 15 GDPR.**

The first case concerned the proper interpretation and application of Article 15(3) which permits a data subject to obtain a “copy” of their personal data, among other things. The second case concerned whether the right of access includes the right to receive the identity of the controller’s employees who are processing the data subject’s personal data in the scope of their employment.

For further information: [C-487/21](#); [C-579/21](#)

---

12/13/2022 – [European Commission](#) | [Press Release](#) | [EU-US Data Privacy Framework](#)

**The European Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework.**

The European Commission submitted its draft decision to the EDPB. Then, it will seek approval from a committee composed of representatives of the EU Member States. It should be noted that the

European Parliament has a right of scrutiny over adequacy decisions. Once this procedure is completed, the Commission can proceed to adopting the final adequacy decision.

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

---

12/08/2022 – [Court of Justice of the European Union](#) | [Decision](#) | [Right to be Forgotten](#)

**The Court of Justice of the European Union ruled that the right to inform and the right to be informed cannot be taken into account where a part – which is not minor in relation to the content as a whole – of the information referred to in the request for dereferencing proves to be inaccurate.**

The decision was rendered by the CJEU following a German case where the applicants requested a company, as the controller of personal data processed by the search engine, to dereference some information found online that they deemed to be inaccurate. The company refused to comply with that request arguing that it was unable to decide whether the information referenced was accurate or not.

For further information: [CJEU Website](#)

---

12/07/2022 – [Court of Justice of the European Union](#) | [Decision](#) | [Judicial Proceedings](#)

**The Court of Justice of the European Union ruled that the action against a decision of the European Data Protection Board was inadmissible.**

According to the Court, the EDPB decision may be challenged before a national court hearing an action against the subsequent final decision that closes the procedure and is adopted at national level.

For further information: [CJEU Website](#)

---

12/06/2022 – [Council of the European Union](#) | [Press Release](#) | [Artificial Intelligence Act](#)

**The Council has adopted its general approach on the Artificial Intelligence Act which aims to ensure that artificial intelligence (AI) systems placed and used in the European Union market are safe and respect existing law on fundamental rights and Union values.**

As a reminder, the Council of the European Union published, on 3 November 2022, the final version of the compromise text on the Proposal for the AI Act.

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

11/16/2022 – [European Commission](#) | [Press Release](#) | [Digital Services Act](#)

**Following its publication in the EU’s Official Journal on 27 October 2022, the European Commission announced that the Digital Services Act (DSA) is now in force**

Most provisions will apply from 17 February 2024. As a reminder, online platforms have until 17 February 2023 to report the number of active end users on their websites. The European Commission will then assess whether a platform should be designated a very large online platform or search engine, which will increase its obligations. Following the European Commission’s designation, the entity in question will have four months to comply with the obligations under the DSA.

For further information: [European Commission Website](#); [DSA Regulation](#)

---

11/14/2022 – [European Data Protection Board](#) | [Recommendations](#) | [Binding Corporate Rules](#)

**The European Data Protection Board published its draft Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules, which are opened for public consultation until 10 January 2023.**

The Recommendations aim to update the former Article 29 documents (WP 256 rev.01), in particular to include Schrems II requirements such as transfer impact assessment and government access requests.

For further information: [EDPB Website](#)

---

11/07/2022 – [European Commission](#) | [Proposal](#) | [Accommodation Rental Services](#)

**The European Commission announced that it adopted a proposal for a regulation on data collection and sharing relating to short-term accommodation rental services.**

The Proposal aims to harmonize and improve the framework for data generation and data sharing on short-term accommodation rentals across the European Union, and to enhance transparency in this sector.

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

---

11/03/2022 – [European Union Agency for Cybersecurity](#) | [Report](#) | [Cybersecurity](#)

**The ENISA published a Threat Landscape 2022 which describes top threats, relevant trends, threat actors and attack techniques, as well as impact and motivation analysis.**

The ENISA outlines that prime threats include ransomware, malware, social engineering threats, threats against data, threats against availability (denial of service threats and internet threats), disinformation or misinformation and supply-chain attacks.

For further information: [European Union Agency for Cybersecurity](#)

---

10/31/2022 – [European Commission](#) | [Press Release](#) | [Digital Markets Act](#)

**The Digital Markets Act (DMA) entered into force on the 1st of November 2022.**

The European Commission outlined that the DMA will start to apply as of 2 May 2023. Then, within two months and at the latest by 3 July 2023, potential gatekeepers will have to notify their core platform services to the Commission if they meet the thresholds established by the DMA.

For further information: [European Commission Website](#); [DMA Regulation](#)

---

10/27/2022 – [Court of Justice of the European Union](#) | [Decision](#) | [Data Subject Rights](#)

**The Court of Justice of the European Union ruled that when a subscriber of a telephone service operator withdraws his or her consent to be included in the directories of a directory provider, the latter must update its own database to take account of this withdrawal, but also inform of this withdrawal the telephone service operator who has communicated these data to it, as well as the other directory providers to whom it has itself transmitted such data.**

The Court also considered that the directory provider must inform search engine providers of the data subject's request for erasure.

For further information: [CJEU Website](#)

---

10/21/2022 – [European Data Protection Board](#) | [Guidelines](#) | [Lead Supervisory Authority](#)

**The European Data Protection Board published its updated Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, which was open for public consultation until December 2nd, 2022.**

The EDPB intends to clarify the notion of main establishment in the context of joint controllership and take into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. The relevant paragraphs have been revised and updated, while the rest of the document is unchanged, except for editorial changes.

For further information: [EDPB Website](#)

---

10/20/2022 – [Court of Justice of the European Union](#) | [Decision](#) | [Data Retention](#)

## **The Court of Justice of the European Union interpreted purpose and storage limitation principles under the GDPR.**

The Hungarian Supervisory Authority imposed a fine of HUF 100,000,000 (approximately €248,000) on the leading internet and broadcasting service providers in Hungary for creating a database test in order to fix technical failures and not immediately deleting it after performing the necessary tests and fixing the flaw. As a result, a large amount of personal data was kept in this database without any purpose for almost 18 months, in a file that could allow the identification of data subjects.

The CJEU ruled that the principle of purpose limitation does not prevent the registration and storage by the data controller in a database created for the purpose of carrying out tests and correcting errors, of personal data previously collected and stored in another database, if such further processing is compatible with the specific purposes for which the personal data was initially collected. However, the principle of storage limitation prevents the controller from storing personal data previously collected for other purposes in a database created for the purpose of carrying out tests and correcting errors, for a period of time longer than that necessary for carrying out said activities.

For further information: [CJEU Website](#) [FR]

---

10/18/2022 – [European Data Protection Board](#) | [Guidelines](#) | [Data Breach](#)

## **The European Data Protection Board published its updated Guidelines 9/2022 on personal data breach notification under the GDPR, which was open for public consultation until 29 November 2022.**

The EDPB intends to clarify the notification requirements concerning the personal data breaches at non-EU establishments. The relevant paragraphs have been revised and updated, while the rest of the document is unchanged, except for editorial changes.

For further information: [EDPB Website](#)

## Belgium

12/15/2022 – [Belgian Official Gazette](#) | [Law](#) | [Whistleblowing](#)

**The Belgian law implementing the EU Whistleblower Directive was published on 15 December 2022 in the Official Gazette and will enter into force on 15 February 2023.**

The law covers the private sector (a separate legislation for the public sector is still being drafted).

For further information: [Belgian Official Gazette](#)

---

## Denmark

10/27/2022 – [Danish Supervisory Authority](#) | [Decision](#) | [Cookies](#)

**The Danish Supervisory Authority published its decision issued on 30 September 2022, in which it had expressed criticism against an online marketing solutions provider’s processing of information about website visitors.**

The Authority expressed serious criticism regarding a website’s consent mechanism which presented a “first layer” with an “Accept all” option which did not give information about all processing purposes. Information about the preferential purpose only appeared in the “second layer” of the consent mechanism, which the visitors could access by clicking on “Customize Settings”.

For further information: [Datatilsynet Website](#) [DK]

---

## Finland

12/20/2022 – [Finnish Official Gazette](#) | [Law](#) | [Whistleblowing](#)

**The Finnish law implementing the EU Whistleblower Directive entered into force on 1 January 2023.**

For further information: [Ministry of justice Website](#)

---

12/14/2022 – [Finnish Supervisory Authority](#) | [Sanction](#) | [Health Data](#)

**The Finnish Supervisory Authority issued a €230,000 fine against a Finnish maritime company for violations related to the processing of employees' health data.**

In particular, the Authority considered that health information must be kept separately from other information about the employee and care must be taken to ensure that the information is correct and deleted as soon as they are no longer needed.

For further information: [Finnish DPA Website](#)

---

## France

12/29/2022 – [French Supervisory Authority](#) | [Sanction](#) | [Cookies](#)

**On December 29, 2022, the French Supervisory Authority issued a €5 million fine against a technology company due to its cookie practices.**

The Authority considered that as several clicks were necessary to refuse all cookies, it amounted to discouraging users from refusing cookies and encouraging them to favor the "accept all" button. In addition, the Authority considered that users were not informed in a sufficiently precise manner of the purposes of cookies. The Authority concluded that such practices constituted a violation of Article 82 of the French Data Protection Act.

For further information: [CNIL Website \[FR\]](#)

---

12/22/2022 – [French Supervisory Authority](#) | [Sanction](#) | [Cookies](#)

**The French Supervisory Authority issued a €60 million fine, on 19 December 2022, against a company which operates and develops a search engine, in particular for not allowing its users to refuse cookies as easily as accepting them.**

The Authority considered that the Company had breached the French Data Protection Act as cookies were set without prior consent of the user, including cookies with an advertising purpose. Also, while the search engine offered a button to accept cookies immediately, it did not offer an equivalent solution to allow the Internet user to refuse them as easily. The Authority specified that two clicks were needed to refuse all cookies, while only one was needed to accept them.

For further information: [CNIL Website](#)

---

12/20/2022 – [French Supervisory Authority | GDPR Application | Dismissal](#)

**On 20 December 2022, the French Supervisory Authority dismissed a sanction procedure initiated against an American company considering that the GDPR was not applicable in this case.**

The Authority considered that the evidence was insufficient to establish the applicability of the GDPR. The establishment criterion provided by article 3 (1) of the GDPR and the targeting criterion provided by article 3 (2) of the GDPR were not met.

For further information: [CNIL Website \[FR\]](#)

---

12/08/2022 – [French Supervisory Authority | Sanction | GDPR Violations](#)

**The French Supervisory Authority issued a €300,000 fine, on 30 November 2022, against a French phone operator, in particular for not respecting the rights of data subjects and the security of its users' data.**

The Authority found several infringements, in particular regarding the company's failure to respect the rights of data subjects (right of access and right to erasure), to ensure the security of personal data (weak passwords, storage and transmission of passwords in clear text) and to comply with the obligation to document a personal data breach.

For further information: [CNIL Website](#)

---

12/05/2022 – [French Supervisory Authority | Guidance | Customer Lists](#)

**The French Supervisory Authority has published a guide on the sale of customer lists.**

The Authority specifies that the file sold to the purchaser must only contain data of active customers who have not objected or who consented to the transmission of their personal data (depending on the means of prospecting). The purchaser will have to inform the individuals (unless they have already been informed), verify the customers consent and, respect the rights of data subjects.

For further information: [CNIL Website \[FR\]](#)

---

11/29/2022 – [French Supervisory Authority | Sanction | Data brokers](#)

**The French Supervisory Authority issued a €600,000 fine, on 24 November 2022, against the first electric utility in France for failure to comply with its obligations regarding commercial prospecting, data subject rights and security of personal data.**

In particular, the Authority found that the company launched a commercial prospecting campaign by electronic means based on data provided by a data broker. However, the prospects were not provided with the list of partners, including the company, at the time they gave their consent. Also, the company admitted that it did not conduct any audits of the data brokers and did not verify the consent forms used by the data brokers. The Authority also considered that the company did not inform data subjects on the data retention periods, as well as the source of the data collected, and also found infringements regarding the implementation of data subject rights and the security of personal data.

For further information: [CNIL Website](#)

---

11/28/2022 – [French Regulatory Authority for Audiovisual and Digital Communication | Charter | Child Influencers](#)

**The French Regulatory Authority for Audiovisual and Digital Communication (ARCOM) published a Charter in which operators of online platforms commit to facilitate the detection and reporting of content harmful to minors, to prevent the commercial processing of their personal data and, to facilitate the implementation of their right to erasure.**

The Charter was taken in application of the Studer law of 19 October 2020 which regulates the commercial exploitation of the image of children under sixteen on online platforms. It should be noted that the French Supervisory Authority will be involved in monitoring the obligations of online platforms arising from the Charter.

For further information: [ARCOM Website \[FR\]](#)

---

11/28/2022 – [French Regulatory Authority for Audiovisual and Digital Communication | Guidelines | Online Content](#)

**The French Regulatory Authority for Audiovisual and Digital Communication (ARCOM) published its Guidelines to prevent the dissemination of hateful content online, highlighting the duties of online and very large online platforms (VLOPs).**

As a reminder, in anticipation of the implementation of the Digital Services Act (DSA), the French legislator has put in place Law No. 2021-1109 of 24 August 2021. The Guidelines aim to clarify the

obligations which result from this law for operators of online platforms reaching 10 million monthly users per month in France, as well as VLOPs which exceed 15 million monthly users.

For further information: [ARCOM Website \[FR\]](#)

---

11/22/2022 – [French Supervisory Authority | Resolutions | Global Privacy Assembly](#)

**The French Supervisory Authority announced that, during its annual meeting in October 2022, the Global Privacy Assembly (composed of data protection and privacy authorities from across the world) adopted two resolutions on cybersecurity and facial recognition.**

For further information: [CNIL Website \[FR\]](#)

---

11/17/2022 – [French Supervisory Authority | Sanction | Data Processing Principles](#)

**The French Supervisory Authority imposed a €800,000 fine, on 10 November 2022, against a French company providing voice over IP (technology that allows users to chat via their microphone and/or webcam over the Internet) and instant messaging services for failing to comply with several obligations of the GDPR, in particular regarding the data retention periods, data protection by default and security of personal data.**

Regarding the company’s failure to ensure data protection by default, it should be noted that the company’s application was set to remain active even when the user closed the main window (by selecting the “X” icon in the upper right corner). Only a small indicator showed that the application was still active. The Authority considered that this setting may lead to users being heard by other members in the voice room when they thought they had left. It was ruled that the company should specifically inform users by making them aware that they are still being heard by others.

For further information: [CNIL Website](#)

---

11/04/2022 – [French Supervisory Authority | Frequently Asked Questions | Cookies](#)

**The French Supervisory Authority updated a series of frequently asked questions about its amended Guidelines and Recommendations on cookies.**

For further information: [CNIL Website \[FR\]](#)

---

10/21/2022 – [French Council of State](#) | [Decision](#) | [Data Protection Officer](#)

**The French Council of State confirmed the French Supervisory Authority’s decision and ruled that the requirement to protect the functional independence of a data protection officer (DPO) does not prevent its dismissal, insofar as the GDPR is not intended to govern the working relationship between the DPO and the employer.**

In particular, the Court ruled that the dismissal of a DPO may be lawful due to deficiencies in the performance of its duties such as failure to respond to other employee’s requests, repeated alerts of non-conformity that are not justified and not documented, as well as failure to comply with the company’s internal regulations.

For further information: [Council of State Website](#) [FR]

---

10/20/2022 – [French Supervisory Authority](#) | [Sanction](#) | [Facial Recognition](#)

**The French Supervisory Authority issued a 20 million euros fine, on 17 October 2022, against a company’s AI facial recognition software for several breaches of the GDPR.**

The Authority also ordered it stop collecting and processing data of individuals residing in France without a legal basis and to delete data of these persons that it had already collected, within a period of two months. The Authority added to this injunction a penalty of 100,000 euros per day of delay beyond these two months.

For further information: [CNIL Website](#)

---

10/18/2022 – [French Official Journal](#) | [Decree](#) | [Retention of Traffic and Location Data](#)

**The Decree No. 2022-1327 of October 17, 2022 ordering, in view of the serious and current threat to national security, the retention of certain categories of connection data for a period of one year has been published in the French Official Journal.**

The decree requires electronic communications operators as well as the persons mentioned in article 6. I. 1) and 2) of the Law No. 2004-575 of June 21, 2004 on Confidence in the Digital Economy to keep traffic and location data for a period of one year.

For further information: [Decree](#) [FR]

---

10/17/2022 – [French Supervisory Authority | Recommendations | Passwords](#)

**The French Supervisory Authority has updated its recommendation regarding passwords.**

The Authority’s recommendation is an update to its 2017 recommendation to reflect evolving knowledge. It aims to define the minimum technical and organizational requirements for authentication by password or by any other non-shared secret (except for cryptographic keys and secrets) implemented in the context of personal data processing.

For further information: [CNIL Website \[FR\]](#)

---

10/14/2022 – [French Official Journal | Decree | Marketing Calls](#)

**The new rules regarding unsolicited marketing telephone calls will enter into force on March 1st, 2023.**

The Decree notably determines the conditions (days, hours and frequency) under which companies may call consumers to make commercial offers. Violation of these provisions is sanctioned by an administrative fine of up to €75,000 for an individual and €375,000 for a legal person.

For further information: [Decree \[FR\]](#)

---

## Germany

12/21/2022 – [Baden Württemberg Supervisory Authority | Sanction | Facial Recognition](#)

**The Baden Württemberg Supervisory Authority (LfDI) has opened fine proceedings against a face search engine. The LfDI already requested the search engine to submit a statement and answer a list of questions in 2021, which the LfDI has now received in November 2022.**

The face search engine advertises that it can identify any person by means of facial recognition, personal profiles and a face database and by comparing photos and the biometric data they contain. It asserted in its statement that it only processes publicly available images and that it cannot assign these images to individuals. For data stored by the search engine, there would therefore be no personal reference at all, and no processing of personal data. The Authority opposed these statements because of the “massive threat to the rights and freedoms of citizens, also in Baden-Württemberg”, particularly as the data processing concerned processing of special categories of personal data pursuant to Art. 9 GDPR.

For further information: [LfDI Website \[DE\]](#)

11/30/2022 – [German Data Protection Conference](#) | [Guidance](#) | [Cookies](#)

**The German Data Protection Conference updated its guidance on the Federal Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia.**

In particular, the updated version includes requirements regarding transfers of personal data to third countries, the design of cookie banners, as well as comments on the lawfulness of processing.

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

---

11/29/2022 – [Hamburg Commissioner for Data Protection and Freedom of Information](#) | [Press Release](#) | [EU-US Data Transfers](#)

**The Hamburg Commissioner for Data Protection and Freedom of Information issued a press release regarding the impact of the Executive Order.**

It addresses the problems surrounding EU-US data transfers as brought forward in the Schrems II decision of the Court of Justice of the European Union.

For further information: [Hamburg Commissioner for Data Protection and Freedom of Information Website](#)

---

11/24/2022 – [German Data Protection Conference](#) | [Guidance](#) | [Third Countries](#)

**The Federal Commissioner for Data Protection and Freedom of Information (BfDI) announced the publication of an updated version of the Standard Data Protection Model (SDM 3.0) by the Data Protection Conference (DSK).**

The standard data protection model is a procedure allowing to translate the legal requirements of the GDPR into concrete technical and organizational measures. It is being developed by a sub-group of the DSK.

For further information: [BfDI Website](#)

---

11/18/2022 – [Baden Württemberg Supervisory Authority | Code of Conduct | Data Processors](#)

**The Authority has approved a Code of Conduct for data processors.**

By committing to the "Trusted Data Processor" code of conduct, processors demonstrate that they follow the guidelines set out in the code of conduct and submit to its supervision by a monitoring body accredited by the Authority.

For further information: [LfDI Website \[DE\]](#)

---

11/04/2022 – [Baden Württemberg Supervisory Authority | Guidance | Videos](#)

**The Authority issued guidance on data protection when uploading or embedding videos on websites.**

In particular, the Authority considers that the best privacy-friendly alternative is self-hosting videos.

For further information: [LfDI Website \[DE\]](#)

---

10/01/2022 – [Thüringen Supervisory Authority | 4th Annual Report | Retention Period](#)

**The Authority decided that the obligation to prove that the data subject has given consent does not cease to apply if the data subject requests the deletion of all personal data.**

The decision was based on article 17 (3) (b) of the GDPR, which precludes the deletion of personal data when it is necessary to comply with a legal obligation. According to the decision, this includes the documentation obligations set out in article 5 (2) and article 7 (1) GDPR.

For further information: [Annual Report \[DE\]](#)

---

09/20/2022 – [Berlin Supervisory Authority | Sanction | Data Protection Officer](#)

**The Berlin Supervisory Authority issued a €525,000 fine against a company due to a conflict of interest of the company's data protection officer.**

A conflict of interest is regularly assumed if the data protection officer simultaneously has a function in the company in which he determines the purposes and means of processing personal data and therefore is supposed to monitor himself. In this case, the data protection officer was also managing director of two service companies which were acting as processors of the company where he was

appointed as data protection officer. The fact that the data protection officer had to monitor the two data processing agreements concerning the companies over which he had influence was considered sufficient for a sanctionable conflict of interest.

For further information: [BlnBDI Press Release \[DE\]](#)

---

## Greece

11/11/2022 – [Greek Official Gazette](#) | [Law](#) | [Whistleblowing](#)

**The new whistleblower protection law adopted by Greece to implement the EU Whistleblower Directive (2019/1937) into national law was published in the Official Gazette.**

For further information: [Greek Official Gazette](#)

---

## Ireland

12/31/2023 – [Irish Supervisory Authority](#) | [Sanction](#) | [GDPR Obligations](#)

**On 4 January 2023, the Irish Supervisory Authority announced the conclusion of two inquiries related to the data processing operations of a social media company in a decision dated 31 December 2022. The Authority fined the company a total of €390 million.**

Following the consultation of concerned supervisory authorities and the European Data Protection Board, the Authority found that the company was not entitled to rely on the newly changed contractual legal basis in connection with the delivery of behavioral advertising as part of its services, and that its processing of users' data to date, in purported reliance on the contractual legal basis, amounted to a contravention of article 6 of the GDPR. The company has also been directed to bring its data processing operations into compliance within a period of 3 months.

For further information: [DPC Website](#)

---

12/23/2022 – [Irish Supervisory Authority](#) | [Inquiry](#) | [Disclosure of Collated Datasets](#)

**The Irish Supervisory Authority launched an inquiry into a social media relating to collated datasets, containing personal data relating to approximately 5,4 million users worldwide of the social media, which had been made available on the internet.**

The datasets mapped the social media's IDs to email addresses and/or telephone numbers of the associated data subjects.

For further information: [DPC Website](#)

---

11/28/2022 – [Irish Supervisory Authority](#) | [Sanction](#) | [Data Scraping](#)

**The Irish Supervisory Authority fined a social media company €265 million, on 25 November 2022, for breaches relating to the public disclosure of collated dataset of data subjects using its services.**

The Authority began this inquiry following media reports about the discovery of a collated dataset of the social media's personal data that had been made available on the internet. The material issues in this inquiry related to compliance to data protection by design and default obligations. In addition to the fine, the Irish Supervisory Authority issued a reprimand and ordered the company to take specified remedial actions.

For further information: [DPC Website](#)

---

11/07/2022 – [Irish Supervisory Authority](#) | [Draft Decision](#) | [GDPR Obligations](#)

**The Irish Supervisory Authority announced submitting a draft decision on a search engine regarding which other concerned supervisory authorities could send any relevant and reasoned objections until 24 November 2022.**

As a reminder, in August 2019, the Irish Supervisory Authority commenced an inquiry into the search engine to examine its compliance with requirements to provide transparent information to data subjects.

For further information: [DPC Website](#)

---

10/10/2022 – [Irish Supervisory Authority](#) | [Guidelines](#) | [Data Subject Access Requests](#)

**The Irish Supervisory Authority announced publishing Guidelines on data subject access requests for controllers.**

The Irish Supervisory Authority answers practical questions including about the deadlines to respond to an access request, the procedure that must be followed by a controller and when a controller can refuse to take action on the request.

For further information: [DPC Website](#)

## Italy

12/22/2022 – [Italian Supervisory Authority](#) | [Sanction](#) | [Accurate data](#)

**The Italian Supervisory Authority published its decision, dated 24 November 2022, imposing a €1 million fine on an electricity company for violating the principles of accuracy and storage limitation and for failing to respond to data subjects' requests.**

For further information: [Garante Website \[IT\]](#)

---

12/19/2022 – [Italian Supervisory Authority](#) | [Sanction](#) | [Employee Monitoring](#)

**The Italian Supervisory Authority published its decision, dated December 1st, 2022, imposing a €100,000 fine on a company for illegally checking employees' emails.**

The Authority also prohibited the company from any further processing of metadata relating to the use of employees' e-mails and ordered the deletion of those unlawfully collected.

For further information: [Garante Website \[IT\]](#)

---

12/05/2022 – [Italian Supervisory Authority](#) | [Sanction](#) | [GDPR Violations](#)

**The Italian Supervisory Authority published its decision, dated 6 October 2022, imposing a €2 million fine on a global social network of voice chats, operated by a US company not established in the EU, for various GDPR violations.**

The Authority found several GDPR infringements, including indefinite retention periods, a lack of transparency, as well as the profiling and sharing of account information without the identification of an appropriate legal basis.

For further information: [Garante Website \[IT\]](#)

---

11/28/2022 – [Italian Supervisory Authority](#) | [Sanction](#) | [GDPR Violations](#)

**The Italian Supervisory Authority published its decision, dated 20 October 2022, imposing a fine of €1,4 million on a company regarding various GDPR violations.**

The Authority found several infringements to the GDPR, including collecting a single consent from data subjects for the general terms and conditions of sale, the privacy notice and the cookie policy.

For further information: [Garante Website \[IT\]](#)

---

11/28/2022 – [Italian Supervisory Authority](#) | [Sanction](#) | [Information](#)

**The Italian Supervisory Authority published its decision, dated 10 November 2022, imposing a fine of €500,000 on a telecommunications company, in particular for violating the GDPR principles of accuracy and transparency in relation to the conclusion of a contract for telephone services.**

For further information: [Garante Website \[IT\]](#)

---

10/18/2022 – [Italian Supervisory Authority](#) | [Investigation](#) | [Cookie Walls](#)

**The Italian Supervisory Authority announced continuing its investigation into online newspapers using cookie walls.**

The investigations concern online newspapers which condition access to content upon a paying subscription or, alternatively, the consent from users to cookies and other tracking tools on their terminals.

For further information: [Garante Website \[IT\]](#)

---

10/12/2022 – [Italian Supervisory Authority](#) | [Investigation](#) | [Artificial Intelligence](#)

**The Italian Supervisory Authority announced that it has opened an investigation regarding an application that converts text files into voice using fake (however realistic) voices of well-known personalities.**

For further information: [Garante Website \[IT\]](#)

---

## Portugal

12/12/2022 – [Portuguese Supervisory Authority](#) | [Sanction](#) | [GDPR Violations](#)

**The Portuguese Supervisory Authority published a decision imposing a fine of €4,3 million to an American institute of research for violating several GDPR requirements.**

The Authority considered that the Institute unlawfully processed personal data relating to health and religion, failed to comply with transparency requirements, breached its duties of diligence in choosing its subcontractors and infringed the legal provisions relating to international data transfers, including the obligation to carry out an impact assessment.

For further information: [CNPD Website](#) [PT]

---

## Spain

12/12/2022 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Data Breach](#)

**The Spanish Supervisory Authority fined a telecommunications company €70,000 (subsequently reduced to €56,000), on 23 September 2022, for failing to take the necessary precautionary measures to ensure a duplicate SIM card was not given to a third party.**

The company provided a duplicate of their SIM card to a third party, without the complainant's consent and without verifying the identity of the third party and, as a result, such third party accessed the complainant's bank details, carried out several fraudulent transactions, and also accessed the complainant's Gmail account.

For further information: [AEPD Website](#) [ES]

---

11/15/2022 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Security](#)

**The Spanish Supervisory Authority fined a bank €100,000 (reduced to 80,000 €) for a security incident caused by a lack of adequate technical and organizational measures.**

A customer of the bank was allowed to access the personal data (account number and account movements) of another customer when he accessed his own bank account.

For further information: [AEPD Website](#) [ES]

---

11/03/2022 – [Spanish Supervisory Authority](#) | [Sanction](#) | [GDPR Violations](#)

**The Spanish Supervisory Authority issued a €70,000 fine against a delivery company for violating the principles of integrity and confidentiality and failing to adopt the necessary security measures to guarantee the protection of its clients' personal data.**

For further information: [AEPD Website](#) [ES]

---

11/02/2022 – [Spanish Supervisory Authority](#) | [Sanction](#) | [GDPR Violations](#)

**The Spanish Supervisory Authority imposed a €525,000 fine on a Spanish media company (adult content) for various GDPR violations, including lack of transparency and fairness.**

In particular, the Authority found that the information provided in the privacy policy of the websites did not reflect the processing actually carried out. The Authority also considered that there was a real risk for minors to have a direct and unrestricted access to harmful content, due to clearly insufficient limitations or safeguards provided on the websites.

For further information: [AEPD Website](#) [ES]

---

10/24/2022 – [Spanish Supervisory Authority](#) | [Advisory Tool](#) | [Data Breach](#)

**The Spanish Supervisory Authority presented its advisory tool to help data controllers assess their obligation to notify a personal data breach to the Spanish Supervisory Authority.**

For further information: [AEPD Website](#) [ES]

---

10/09/2022 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Security](#)

**The Spanish Supervisory Authority issued a €80,000 fine (reduced to €48,000) to a provider of technological infrastructure management services for publishing the personal data of clients of an insurance company on different forums.**

For further information: [AEPD Website](#) [ES]

---

## Sweden

10/31/2022 – [Administrative Court of Stockholm](#) | [Decision](#) | [Art 77 GDPR](#)

**The Stockholm Administrative Court (FiS) held that Swedish law does not deny complainants under Article 77 GDPR to have a status of party. This also applies if the supervisory authority opened a parallel ex officio investigation into a similar matter and the same company.**

For further information: [FiS Ruling \[SWE\]](#)

---

## United Kingdom

12/12/2022 – [UK Supervisory Authority](#) | [Sanction](#) | [Marketing](#)

**The UK Supervisory Authority issued a £70,000 (approx. €79,000) fine to a company for sending more than 400,000 unsolicited direct marketing SMS to subscribers who had not consented to receiving them.**

For further information: [Monetary Penalty Notice](#)

---

12/12/2022 – [UK Supervisory Authority](#) | [Sanction](#) | [Marketing](#)

**The UK Supervisory Authority issued a £125,000 (approx. €142,000) fine to a company for sending around 3,500,000 direct marketing emails and text messages to individuals who had not given valid consent.**

For further information: [Monetary Penalty Notice](#)

---

12/07/2022 – [UK Supervisory Authority](#) | [Sanction](#) | [Marketing Calls](#)

**The UK Supervisory Authority fined five companies a total of £435,000 (approx. €495,000) for making nearly half a million unlawful marketing calls to individuals registered in the national opt out service.**

For further information: [ICO Website](#)

---

11/23/2022 – [UK Government](#) | [Regulation](#) | [Data Transfers](#)

**The UK Government has formalized its first post-Brexit adequacy decision, with the Republic of Korea.**

The ‘data bridge’ (the UK Government’s new term for adequacy decisions), which enters into force on December 19, 2022, has a broader scope than the existing EU adequacy decision recognizing South Korea.

For further information: [Government Website](#)

---

11/17/2022 – [UK Supervisory Authority](#) | [Guidance](#) | [Data Transfers](#)

**The UK Supervisory Authority announced the publication of an update to its guidance on international transfers, including a new section on transfer risk assessments (TRAs) and a TRA tool.**

For further information: [ICO Website](#)

---

10/26/2022 – [UK Supervisory Authority](#) | [Reports](#) | [Biometric Data](#)

**The UK Supervisory Authority published two reports to warn organizations against immature biometric technologies which could be discriminating against people.**

For further information: [ICO Website](#)

---

10/24/2022 – [UK Supervisory Authority](#) | [Sanction](#) | [Security](#)

**The UK Supervisory Authority imposed a fine of £4,400,000 (approx. €5,000,000), on 19 October 2022, on a construction company for failing to process personal data in a manner that ensured appropriate security of the personal data using appropriate technical and organizational measures as required by the GDPR.**

For further information: [ICO Website](#)

---

10/17/2022 – [UK Supervisory Authority](#) | [Guidance](#) | [Direct Marketing](#)

**The UK Supervisory Authority updated its guidance on direct marketing using electronic mail.**

The guidance details what is required to comply with the Privacy and Electronic Communications Regulations 2003 (PECR), including what electronic mail marketing is and how to comply with rules on direct marketing. It also discusses the relationship between the PECR and data protection regulations.

For further information: [ICO Website](#)

---

10/12/2022 – [UK Supervisory Authority](#) | [Draft Guidance](#) | [Employee Monitoring](#)

**The UK Supervisory Authority published detailed draft guidance on monitoring at work and data protection.**

The Authority provides guidance for employers on their legal obligations, under the UK GDPR and the Data Protection Act 2018, regarding the monitoring of workers and addresses specific types of monitoring (e.g., automated processes in monitoring tools, and the use of audio, video or biometric data to monitor workers).

For further information: [ICO Website](#)

---

10/12/2022 – [National Cyber Security Centre](#) | [Guidance](#) | [Cyber Attacks](#)

**The National Cyber Security Centre issued guidance to better help organizations to assess the cyber security level of their supply chain.**

For further information: [National Cyber Security Centre Website](#)

---

10/04/2022 – [UK Supervisory Authority](#) | [Guidance](#) | [Marketing](#)

**The UK Supervisory Authority updated its guidance on direct marketing using live calls.**

For further information: [ICO Website](#)



# GIBSON DUNN

*This newsletter has been prepared by the EU 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](mailto:abaladi@gibsondunn.com))
  - **Vera Lukic** – Partner, Paris ([vlukic@gibsondunn.com](mailto:vlukic@gibsondunn.com))
  - **Kai Gesing** – Partner, Munich ([kgesing@gibsondunn.com](mailto:kgesing@gibsondunn.com))
- **Joel Harrison** – Partner, London ([jharrison@gibsondunn.com](mailto:jharrison@gibsondunn.com))
  - **Alison Beal** – Partner, London ([abeal@gibsondunn.com](mailto:abeal@gibsondunn.com))
- **Clémence Pugnet** – Associate, Paris ([cpugnet@gibsondunn.com](mailto:cpugnet@gibsondunn.com))
- **Léna Bionducci** – Associate, Paris ([lbionducci@gibsondunn.com](mailto:lbionducci@gibsondunn.com))
- **Yannick Oberacker** – Associate, Munich ([yoberacker@gibsondunn.com](mailto:yoberacker@gibsondunn.com))

© 2023 Gibson, Dunn & Crutcher LLP

*Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.*