GIBSON DUNN

October 13, 2022

GIBSON DUNN | EUROPE | PRIVACY CYBERSECURITY DATA INNOVATION - Q3 2022

To Our Clients and Friends:

Personal Data | Cybersecurity | Data Innovation

Europe

10/07/2022 – United States Government | Executive Order | EU-US Data Transfers

President Biden signed an Executive Order to implement the EU-US Data Privacy Framework, aiming to safeguard cross-border data flows.

As a reminder, the Privacy Shield framework (which used to enable transfers of personal data from the EU to the US) was declared invalid by the Court of Justice of the European Union in 2020 (*Schrems II ruling*). In March 2022, leaders of the EU and the US announced that they agreed "in principle" to a new trans-Atlantic data flow agreement (the EU-US Data Privacy Framework). For that purpose, the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities directs the steps that the US will take to implement the US commitments under the EU-US Data Privacy Framework.

The Framework notably aims to provide binding safeguards to limit US intelligence authorities access to data to what is necessary and proportionate to protect national security. A Data Protection Review Court will also be created to investigate and resolve complaints of Europeans on access of data by US intelligence authorities.

The White House asserts that this will provide the European Commission with a basis to adopt a new adequacy determination, but also greater legal certainty for companies using Standard Contractual Clauses to transfer personal data to the US.

For further information: White House Website

09/20/2022 – Court of Justice of the European Union | Decision | Data Retention

The Court of Justice of the European Union ruled that the general and indiscriminate retention of traffic data by operators providing electronic communications services for a year in order to combat market abuse offences including insider dealing is not compliant with European law.

However, in case of a serious threat to national security, some personal data (such as traffic and location data or IP addresses) may be retained under certain circumstances.

For further information: CJEU Website

09/15/2022 – European Commission | Regulation | Cybersecurity

The European Commission has presented its proposal for a new Cyber Resilience Act. The aim of the proposal is to protect both consumers and businesses from products with inadequate security features and thereby ensure a better level of cybersecurity.

In particular, the Cyber Resilience Act draft introduces mandatory cybersecurity requirements and obligations for manufacturers, as well as importers and distributors, of products with digital elements (i.e., software or hardware product and its remote data processing solutions, defined as any data processing at a distance for which the software is designed and developed by the manufacturer or under its responsibility and the absence of which would prevent the product from performing one of its functions) within the European Union. Any vulnerability contained in the product or any incident impacting its security will have to be reported by the manufacturer to the European Union Agency for Cybersecurity (ENISA). The "critical products" (e.g., operating systems, firewalls or network interfaces) would be subject to a specific compliance procedure.

This proposal of Regulation, if adopted, will be directly applicable in all Member States. Sanctions for violation will depend on the concerned breach (up to €15 million or 2.5% of the company's total worldwide annual turnover of the preceding financial year, whichever is the higher).

In terms of timeline, it still has to be examined by the European Parliament and the Council and, once adopted, companies will have two years to adapt to the new requirements (one year for reporting obligations of manufacturers of incidents/vulnerabilities — *if not modified in the final version of the Regulation)*.

For further information: European Commission Website

08/01/2022 – Court of Justice of the European Union | Decision | Special Categories of Data

The Court of Justice of the European Union ruled that indirectly revealing the sexual orientation of a natural person constitutes processing of special categories of personal data, protected under Article 9 of the GDPR.

In this case, Lithuanian legislation provided for the online publication of the declaration of private interests, required from individuals working in the public service in order to prevent corruption. This

declaration contained name-specific data relating to the individual's spouse, cohabitee or partner, thus disclosing indirectly his/her sexual orientation.

For further information: CJEU Website

07/28/2022 – European Data Protection Board and European Data Protection Supervisor | Joint Opinion | Child Sexual Abuse

The European Data Protection Board and the European Data Protection Supervisor adopted a Joint Opinion 04/2022 on the Proposal for a regulation to prevent and combat child sexual abuse.

In particular, the Opinion stresses the concerns regarding the proportionality of the interferences and limitations to the protection of the fundamental rights to privacy and the protection of personal data.

For further information: EDPB Website

07/18/2022 – European Union | Regulation | Digital Markets Act

The Council of the European Union gave its final approval to the Digital Markets Act.

Following the signature of the Digital Markets Act by the President of the European Parliament and the President of the Council, it will apply six months after publication in the Official Journal of the European Union.

For further information: Council of the European Union

07/14/2022 – European Data Protection Board | Document | Cooperation

In order to enhance cooperation between European supervisory authorities, the Board has published a set of criteria for identifying cross-border cases of strategic importance in different Member States, as well as the process followed by the Board to select these cases.

The Commission recalls that cases of strategic importance are primarily one-stop-shop cases which are likely to involve a high risk to the rights and freedoms of individuals in several Member States. In particular, several criteria have been defined by the Council (e.g., cases related to the intersection of data protection and other legal fields, where a high risk can be assumed, where a data protection impact assessment is required or where there is a large number of complaints in several Member States).

The supervisory authorities may refer to other supervisory authorities in any case that meets at least one of the criteria. The Board members will then decide which cases will be identified as cases of strategic

importance at the European level. The Board already agreed on three (undisclosed) cases to start the project.

For further information: EDPB Website

07/12/2022 – European Data Protection Board and European Data Protection Supervisor | Joint Opinion | European Health Data Space

The European Data Protection Board and the European Data Protection Supervisor adopted a Joint Opinion 03/2022 on the European Commission's Proposal for a Regulation on the European Health Data Space.

The Opinion aims to draw attention to a number of overarching concerns such as the clarification of the interplay between the Proposal and the GDPR or Member State laws.

For further information: Joint Opinion

07/12/2022 – European Data Protection Board | Statement | Data Transfers

The Board adopted a Statement on data transfers to Russia.

The Board recalls that data exporters who transfer personal data to Russia should assess and identify appropriate safeguards and the necessity for supplementary measures to ensure that data subjects are afforded a level of protection that is essentially equivalent to that guaranteed within the EU.

For further information: EDPB Website

Belgium

09/07/2022 – Belgian Supervisory Authority | Preliminary Questions | Advertising

The Belgian Supervisory Authority announced it has referred preliminary questions to the Court of Justice of the European Union (CJEU) regarding the appeal filed by IAB Europe in the case against the compliance of the so-called Transparency & Consent Framework (TCF) with the GDPR.

As a reminder, the TCF aims to contribute to the GDPR compliance of the OpenRTB protocol, which is one of the most widely used Real-Time Bidding protocols. In February 2022, the Belgian Supervisory Authority fined IAB €250.000 on the basis that the TCF infringes the GDPR.

In particular, the CJEU will have to determine whether a transparency and consent string which reflects users' consent, objections and preferences can be considered as personal data.

For further information: CJUE Questions

08/19/2022 – Belgian Supervisory Authority | Sanction | Medical Data

The Belgian Supervisory Authority imposed a €20.000 fine on a medical analysis laboratory regarding various GDPR violations.

The Authority found that the principles of integrity and confidentiality were violated insofar as health data was processed through a website without using encryption. In addition, the argument that a privacy policy was not required on the website used as a "mere commercial showcase" was rejected as it was considered as an important operational tool for the laboratory's activities. Finally, the Authority sanctioned the company for not having carried out a data protection impact assessment despite the fact that a large amount of health data was processed.

For further information: APD Website [NL]

08/17/2022 – Belgian Supervisory Authority | Decision | Complaint

The Belgian Supervisory Authority considered that a company may file a complaint against another one.

According to the Authority, the GDPR does not prohibit national regulations from allowing persons other than data subjects to file a complaint before a supervisory authority, for example where a personal data breach occurs in the context of a business relationship.

For further information: APD Website [NL]

Croatia

07/21/2022 – Croatian Supervisory Authority | Sanction | Security Breach

Following a personal data breach, the Croatian Supervisory Authority fined a company HRK 2.15 million (approx. €285.000) for failure to take adequate technical and organizational security measures.

In particular, the Authority highlighted that no access restrictions had been implemented and considered it an aggravating factor that the company is one of the main telecommunications services providers in Croatia.

For further information: AZOP Website [HR]

Denmark

09/21/2022 – Danish Supervisory Authority | Press Release | Data Transfers

The Danish Supervisory Authority issued a decision against a company using the analytics tool of an American company, reaffirming that said tool cannot be used in accordance with Chapter V of the GDPR without supplementary measures.

As a reminder, the Austrian, French and Italian Authorities expressed similar concerns.

For further information: Datatilsynet Website [DK]

08/18/2022 – Danish Supervisory Authority | Decision | Data Transfers

The Danish Supervisory Authority upheld the ban on a municipality's use of a cloud-based workspace, imposed on July 14, 2022.

The Authority specified that the ban will apply until the municipality brings its processing activities in line with the GDPR and carries out a data protection impact assessment that meets the GDPR requirements.

For further information: Datatilsynet Website [DK]

07/14/2022 – Danish Supervisory Authority | Sanction | Security Breach

The Danish Supervisory Authority proposed to fine a Danish law firm DKK 500.000 (approx. €67.000) for failing to implement appropriate data security measures.

The Authority found that basic security measures (such as multifactor authentication to login to IT systems) were not implemented by the Danish law firm while a large amount of personal data was being processed.

For further information: Datatilsynet Website [DK]

Estonia, Latvia and Lithuania

07/27/2022 – Baltics States Data Supervisory Authorities | Coordination | Short-Term Vehicle Rental

Supervisory Authorities of the Baltic States initiated a coordinated inspection of privacy practices in the field of short-term vehicle rental.

The Estonian, Latvian and Lithuanian Supervisory Authorities launched a coordinated preventive supervision of companies specialized in short-term vehicle rental. The aim is to monitor compliance with the GDPR and to proactively address potential threats to privacy in this sector, in light of its increasing importance in the daily lives of many citizens over the last three years.

For further information: EDPB Website

Finland

07/05/2022 – Finnish Supervisory Authority | Sanction | Data Subject Rights

The Finnish Supervisory Authority published a decision issued on May 9, 2022, imposing a €85.000 fine on a Finnish magazine publisher for deficiencies in the implementation of data subject rights.

In particular, the decision outlines that some of the data subjects' requests were not handled due to a technical issue in the e-mail redirect. In addition, the company gathered an excessive amount of information for identification by requiring data subjects to complete and sign a printable form to identify the customer exercising his/her right, and collecting signatures, without a justified reason (such as comparing the customer's signature with one already in its possession, which was not the case here).

For further information: Ombudsman Website

France

09/08/2022 – French Supervisory Authority | Sanction | Data Security

The French Supervisory Authority fined the French Trade and Companies Register €250.000, for breaches relating to data security and retention periods.

In particular, strong passwords were not required to create a user account and personal data such as passwords were stored and transmitted in clear text. Besides, the data of a quarter of the service's users was kept beyond the retention period.

For further information: CNIL Website [FR]

09/07/2022 – French Government | Regulation | Cybersecurity

A bill proposed various revisions to French legislation, with the aim to act against cybercrime.

In particular, the bill proposes a framework for insurance reimbursement clauses, making such reimbursement conditional on the filing of a complaint by the victim. Besides, in the context of a criminal procedure, and under the authorization given by the official authorities, enforcement authorities may seize digital assets.

For further information: French Senate Website [FR]

08/03/2022 – French Supervisory Authority | Sanction | Marketing Communication

The French Supervisory Authority fined a French group of hotels €600.000 for various breaches in the context of marketing activities.

The group sent marketing messages to customers without their consent, and did not comply with the exercise of data subject's rights. For example, the box to subscribe to a marketing newsletter was pre-ticked, and technical issues prevented individuals from exercising their right to object.

For further information: CNIL Website [FR]

07/26/2022 – French Supervisory Authority | Recommendations | Age Verification Systems

The French Supervisory Authority issued its recommendations for online age verification systems.

In particular, the Authority reminded that pornographic websites shall not directly collect identity documents, estimate a visitor's age based his/her browsing history, nor process biometric data to uniquely identify or authenticate an individual. The Authority further suggested using an independent trusted third party to prevent the direct transmission of identifying data about the user to the website or application publishing pornographic content, in accordance with the data minimization principles.

For further information: CNIL Website [FR]

07/22/2022 – French Administrative Court | Decision | Personal Data Breach Notification

The French Administrative Court (*Conseil d'Etat*) ruled that data controllers are not required to notify a personal data breach to the French Supervisory Authority (CNIL) if the CNIL was already aware of the breach.

On that basis, the *Conseil d'Etat* reduced the fine imposed by the CNIL from €3.000 to €2.500.

For further information: French Administrative Court Website [FR]

07/21/2022 – French Supervisory Authority | Sanction | Geolocation Data

The French Supervisory Authority fined a short-term vehicle rental company €175.000, in particular for having disproportionately infringed the privacy of its customers by geolocating them almost permanently.

The company also failed to identify and implement a proportionate data retention period, and to inform individuals.

For further information: CNIL Website

07/08/2022 – French Supervisory Authority | Formal Notices | Website Security

The French Supervisory Authority issued formal notices against fifteen organizations for insufficiently secured websites, amongst the twenty-one websites inspected in 2021.

The Authority highlights the lack of sufficient data encryption, including obsolete versions of the transport layer security (TSL) protocol and unsecured access (HTTP) to the website, and the lack of sufficient measures to protect users' accounts, such as weak password policies.

For further information: CNIL Website [FR]

Germany

09/21/2022 – Baden Württemberg Supervisory Authority | Sanction | Use of Personal Data from Public Land Register

The Baden Württemberg Supervisory Authority imposed fines of €50.000 against a company and €5.000 against an individual for using personal data from a public land register for business development purposes.

The Authority highlights that there is no legitimate interest to process personal data as the register is created pursuant to a legal obligation, to ensure legal certainty and protect property interests, but not to facilitate marketing.

For further information: BfDI-BW Website [DE]

09/20/2022 – Berlin Commissioner for Data Protection and Freedom of Information | Sanction | Data Protection Officer

The Berlin Supervisory Authority imposed a €525.000 fine on the subsidiary of an e-commerce group because its data protection officer had a conflict of interest.

The Authority highlighted that the appointed data protection officer was the managing director of two service companies that processed personal data on behalf of the company for which he was the data protection officer. The Authority held that the subsidiary failed to comply with the GDPR insofar as a conflict of interest had arisen with no action being taken by the company, despite a previous warning issued in 2021.

For further information: BfDI Website [DE]

09/08/2022 – Lower Saxony Supervisory Authority | Warning | Profiling

The Lower Saxony Supervisory Authority issued a press release warning banks against profiling for advertising purposes.

In particular, payment transaction data and third-party data was used by the bank to assess whether a customer might be interested in a particular product. According to the Supervisory Authority, such processing would be unlawful insofar as legitimate interests of the controller cannot constitute the legal basis for the processing, and the consent forms used did not meet the GDPR requirements.

For further information: LfD Niedersachsen [DE]

09/07/2022 – Karlsruhe Higher Regional Court | Decision | Data Transfers

The Karlsruhe Higher Regional Court overturned the judgment of the Baden-Württemberg Procurement Chamber, which argued that a company had to be excluded from a public procurement procedure as its offer violated Chapter V of the GDPR governing data transfers.

As a reminder, the Baden-Württemberg Procurement Chamber excluded a company from a procurement procedure insofar as the company intended to employ the services of a Luxembourg subsidiary of an

American cloud provider. According to the Baden-Württemberg Procurement Chamber, the mere risk of access to personal data stored in the European Union by American authorities would be considered as a data transfer.

The Regional Court overturned the judgment, considering that the sole group affiliation does not imply that illegal instructions might be received from the American cloud provider. However, the Regional Court did not address the Chamber of Public Procurement's argument that the mere ability to access personal data from outside the European Union by a US cloud provider would be considered a transfer under Chapter V of the GDPR.

For further information: Oberlandesgericht Karlsruhe [DE]

08/18/2022 – Thuringia Data Protection Authority | Recommendation | Data Transfers

The Thuringia Data Protection Authority published a recommendation regarding the dynamic embedding of an American provider's fonts on a website without obtaining visitors' prior consent.

The Authority refers to recent case law regarding the dynamic embedding of fonts, which was found to constitute a data transfer to the US (of at least the IP address of a website visitor) because of the dynamic linking. Instead, the Authority recommends considering hosting these fonts locally to avoid any link to US servers.

For further information: TLfDI Thüringen Website [DE]

08/09/2022 – Federal Institute for Drugs and Medical Devices | Regulation | Data Protection Certification

The Federal Institute for Drugs and Medical Devices has published standard data protection criteria for digital health and care applications, making it one of the first authorities to establish a data protection certification under Article 42 of the GDPR.

For further information: BfArM Website [DE]

07/28/2022 – Lower Saxony Supervisory Authority | Sanction | Profiling

The Lower Saxony Supervisory Authority fined a bank €900.000 for profiling its active and former customers for advertising purposes without their consent.

For further information: LfD Niedersachsen Website [DE]

07/26/2022 – Lower Saxony Supervisory Authority | Sanction | Driver Assistance System

The Lower Saxony Supervisory Authority fined a car company €1.1 million for using a test vehicle with a driver assistance system using a surveillance camera without informing data subjects, conducting a data protection impact assessment, nor entering into an agreement with its processor.

In particular, the Authority highlights that a vehicle equipped with a driver assistance system using surveillance cameras must be equipped with magnetic signs displaying a camera symbol and other required information for the data subjects, in this case other road users.

For further information: LfD Niedersachsen Website [DE]

07/19/2022 – German Supervisory Authorities | Recommendation | Data Processing Agreements

Several German data protection authorities undertook a joint exercise to review model data processing agreements used by website hosting providers for the processing of their customers' personal data.

The German data protection authorities have published a detailed checklist for data processing agreements in this respect.

For further information: BlnBDI Website [DE]

Greece

07/13/2022 – Hellenic Supervisory Authority | Sanction | Facial Recognition

The Hellenic Supervisory Authority fined an American AI company specialized in facial recognition €20 million for multiple breaches of the GDPR.

As a reminder, the company used data scraped from the internet for facial recognition and has already been subject to enforcement actions, including in France, Italy, Australia, the UK and Canada.

The Authority notably highlights that the Company failed to name a representative since the company is not established in the European Union, to lawfully process personal data, to inform the data subject and to ensure the right of access of data subjects.

For further information: HDPA Website [GR]

Ireland

09/15/2022 – Irish Supervisory Authority | Sanction | Protection of Minors

The Irish Supervisory Authority fined a social media company €405 million for breaches relating to the public disclosure of children's personal data using the social media's business features and a public-by-default setting for personal accounts of children.

As the Authority was unable to reach consensus with the concerned supervisory authorities, the European Data Protection Board issued a binding decision in accordance with the GDPR dispute resolution process. In addition to the fine, the Authority imposed a range of corrective measures, including an order to bring the processing into compliance by taking a range of specified remedial actions.

For further information: DPC website; EDPB Binding Decision

07/06/2022 – Irish Supervisory Authority | Reprimand | Erasure Request

The Irish Supervisory Authority published a reprimand issued on April 27, 2022 against a social media company, for requiring data subjects to provide copies of their IDs when submitting erasure requests.

In particular, the Authority found that the company failed to comply with the data minimization principle and to provide a valid legal basis for such processing. It also ordered the company to revise its internal policies and procedures for handling erasure requests.

For further information: DPC Decision

Italy

06/30/2022 – Italian Supervisory Authority | Sanction | Financial Data

The Italian Supervisory Authority published a decision issued on May 26, 2022, imposing a €100.000 fine on an Italian bank for the unlawful disclosure of customer data to an unauthorized third party.

The bank disclosed a data subject's banking activity to its parent company without a valid legal basis. The Authority rejected the bank’s argument according to which the disclosure was made by an employee in good faith.

For further information: Garante Website [IT]

Netherlands

07/27/2022 – Dutch Council of State | Decision | Legitimate Interest

The Dutch Council of State upheld a decision overturning the €575.000 fine imposed by the Dutch Supervisory Authority against a video and social platform in 2020. Besides, the European Commission issued a letter, asking the Authority to change its position according to which pure commercial interest does not qualify as legitimate interest.

As a reminder, the case concerned a video and social media platform that installed streaming cameras around amateur soccer fields. The Authority held that the platform could not use legitimate interest as a legal basis since its interest is exclusively commercial. On the contrary, the district court and the Council of State ruled that the platform has other interests such as the interests of players or the public watching the game.

In its letter, the European Commission considers that the Authority's strict interpretation of legitimate interests is not in line with the GDPR and severely limits businesses' possibilities of processing personal data for commercial interests, as they would have to collect consent from the data subject in every case where an economic interest is pursued. Against this background, the Commission invited the Authority to readjust its position and reflect that commercial interests can be regarded as legitimate interests when they are not overridden by the fundamental rights and freedoms of the data subject.

For further information: Raad van State Website [NL]; European Commission Letter

---

Norway

09/09/2022 – Norwegian Supervisory Authority | Sanction | Credit Assessment

The Norwegian Supervisory Authority published a decision issued on August 25, 2022, imposing a NOK 200.000 (approx. €20.000) fine on a company for performing a credit assessment on a data subject without any legal basis to do so.

The Authority notes that the data subject did not have any kind of customer relationship or other connection with the company. In particular, the Authority found that legitimate interest cannot be used a lawful basis insofar as the data subject did not expect the company to process his credit information.

For further information: Datatilsynet Website [NO]

Poland

07/06/2022 – Polish Supervisory Authority | Sanction | Personal Data Breach Notification

The Polish Supervisory Authority fined a company PLN 15.994 (approx. €3.500) for failing to notify a personal data breach.

The Authority considered that a company who loses an employment certificate must notify such breach, even if the employee does not file a complaint, since the certificate of employment contains personal data (e.g., period of employment, parental and child care leave taken).

For further information: EDPB Website

Portugal

08/16/2022 – Portuguese Supervisory Authority | Sanction | Data Security

The Portuguese Supervisory Authority announced the publication of Law No. 16/2022 of August 16, 2022 which approves the Electronic Communications Law.

The law aims to implement several EU Directives, including the Directive 2018/1972 establishing the European Electronic Communications Code. The law notably requires operators to notify the Authority of any security incident and imposes obligations to ensure an adequate level of security for public electronic communication networks and publicly available electronic communications services. This new law will come into force within 90 days as of its publication.

For further information: ANACOM Website [PT]

Romania

09/08/2022 – Romanian Supervisory Authority | Sanction | Security

The Romanian Supervisory Authority fined a digital and media company RON 39.272 (approx. €8.000) for failure to implement adequate technical and organizational measures.

The Authority found that a security incident impacting the platform managed by the company led to an unauthorized disclosure or access to personal data, including names, telephone numbers and bank data.

For further information: ANSPDCP Website [RO]

08/22/2022 – Romanian Supervisory Authority | Sanction | Security of Processing

The Romanian Supervisory Authority fined an energy company RON 49.337 (approx. €10.000) for failure to implement remedial measures to reduce risk following a personal data breach.

The Authority considered that the company, which sent an email containing personal data to the wrong person, breached Article 32 of the GDPR by not providing the Authority with sufficient information on the remedial measures taken following the incident. In addition, the Authority issued a warning against the company for failing to notify the breach.

For further information: ANSPDCP Website [RO]

08/09/2022 – Romanian Supervisory Authority | Sanction | Transparency

The Romanian Supervisory Authority fined a passenger transportation company RON 34.630,40 (approx. €7.000) for failure to provide clear, complete and accurate information to data subjects.

In particular, the company's website did not provide information regarding the purpose and the legal basis of the processing, the identity and contact data of the data controller, the data retention periods and the conditions for the exercise of data subject's rights.

For further information: ANSPDCP Website [RO]

Slovenia

08/05/2022 – Slovenian Supervisory Authority | Guidance | Data Protection Impact Assessments

The Slovenian Supervisory Authority published a guide for conducting data protection impact assessments (DPIA).

In particular, the guidance highlights common DPIA shortcomings, gives recommendations to data controllers, and provides a checklist to help determine if a DPIA is comprehensive.

For further information: Slovenian Supervisory Authority Website [SL]

Spain

08/04/2022 – Spanish Supervisory Authority | Sanction | Data Accuracy

The Spanish Supervisory Authority fined an electricity company €50.000 for violation of the accuracy principle.

The Authority found that the company breached the principle of accuracy by linking wrong information, and consequently causing the cancellation of the complainant's electricity supply contract with his provider.

For further information: AEPD Website [ES]

08/02/2022 – Spanish Supervisory Authority | Sanction | Lawfulness of Processing – Spanish Supervisory Authority | Sanction | Lawfulness of Processing

The Spanish Supervisory Authority fined a bank €42.000 for violations of the lawfulness of processing principle.

The Authority found that after the claimant asked the bank several times not to send any stock market investment report by post to his home address, the bank continued to do so.

For further information: AEPD Website [ES]

07/26/2022 – Spanish Supervisory Authority | Guidance | Biometric Data

The Spanish Supervisory Authority issued guidance regarding the use of biometric data.

The guidance focuses on data protection impact assessments in relation to biometric data and the criteria used to classify biometric systems in the framework of a processing operation when assessing the risk to the rights and freedoms of individuals that the processing of such data may entail.

For further information: AEPD Website

07/22/2022 – Spanish Supervisory Authority | Sanction | Marketing Calls

The Spanish Supervisory Authority fined a telecommunications company €40.000 for unlawful marketing calls, despite a data subject's registration in the national opt-out list and notification of his direct opt-out to the company.

For further information: AEPD Website [ES]

07/18/2022 – Spanish Supervisory Authority | Sanction | Data Processing Principles

The Spanish Supervisory Authority fined a bank €56.000 for failing to comply with various data processing principles.

In particular, the Authority ruled that the bank violated the principle of integrity and confidentiality of processing by sending a report on a data subject's investment to the wrong recipient, due to a computer error.

For further information: AEPD Website [ES]

07/13/2022 – Spanish Supervisory Authority | Sanction | Personal Data Breach

The Spanish Supervisory Authority published a decision issued on May 3, 2022, imposing a €132.000 fine on an insurance company for repeatedly sending medical data to an unauthorized third party and failing to notify a personal data breach despite being alerted.

For further information: AEPD Website [ES]

Sweden

09/13/2022 – Swedish Supervisory Authority | Decision | Sensitive Personal Data

The Swedish Supervisory Authority sanctioned a company for offering a browsing service that allows users to access court decisions containing sensitive personal data.

In particular, the Authority highlighted that the company's database gave users access to court decisions with information on individuals who had undergone mandatory care due to mental illness or addiction. Therefore, the Authority issued a reprimand and ordered the company to take measures to prevent such access.

For further information: IMY Website [SE]

09/06/2022 – Swedish Supervisory Authority | Investigation | Employee Monitoring

The Swedish Supervisory Authority announced that it has opened an investigation regarding a transport company for monitoring the driving behavior of some of its employees.

The Swedish Supervisory Authority asked the transport company to clarify whether it had a legal basis for processing and whether it had provided required information to its employees.

For further information: IMY Website [SE]

Switzerland

08/31/2022 – Swiss Supervisory Authority | Press Release | New Data Protection Legislation

The Swiss Supervisory Authority announced that a new data legislation will come into force on September 1, 2023.

This regulation aims to improve data protection in Switzerland and shares similarities with the GDPR, such as data processing principles, the obligation to report personal data breaches and to conduct data protection impact assessments. It differs from the GDPR in some respects as, for example, there is no obligation for companies to appoint a data protection officer.

For further information: Swiss Supervisory Authority Website [FR]

08/09/2022 – Swiss Supervisory Authority | Document | Access Request

The Swiss Supervisory Authority issued recommendations on the exercise of access requests.

The Authority published recommendations in a dispute settlement procedure between a the Federal Intelligence Service (FIS) and a claimant requesting access to documents concerning the legal basis and processing of the FIS' facial recognition systems. The FIS refused on the basis of national law, which provides that access to official documents shall be restricted if it jeopardizes the internal or external security of Switzerland. However, the Supervisory Authority deemed the FIS' arguments too general and unspecific to prove a threat to the internal or external security of Switzerland and recommended the FIS to grant the claimant full access to the required documents.

For further information: Swiss Supervisory Authority recommendations [DE]

United Kingdom

09/07/2022 – UK Supervisory Authority | Guidance | Privacy-Enhancing Technologies

The UK Supervisory Authority has published draft guidance on privacy-enhancing technologies (PETs).

The publication forms part of the Authority's draft guidance on anonymization and pseudonymization. The draft guidance explains some of the different types of PETs and their benefits, as well as how they can help organizations comply with data protection law.

For further information: ICO Website

09/06/2022 – UK Supervisory Authority | Sanction | Direct Marketing

The UK Supervisory Authority fined a UK-based motoring and cycling retailer £30.000 (approx. €34.000) for sending unsolicited marketing emails to data subjects without their consent.

The Authority held that the company improperly relied on legitimate interest as a lawful basis and could not count on the soft opt-in exemption insofar as the customers who received the email had opted out of marketing.

For further information: ICO Website

08/19/2022 – UK Supervisory Authority | Guidance | Complaint

The UK Supervisory Authority published guidance for small businesses that receive data protection complaints.

The Authority issued a six-step guide to acknowledge receipt of the complaint, find out the specific issue related to the complaint, provide updates to the data subject, record actions taken in response to the complaint, formally respond to the individual regarding the outcome of the investigation, and review the lessons learned.

For further information: ICO Website

07/21/2022 – UK and US Government | Joint Statement | Data Access Agreement

UK and US Governments issued a joint statement announcing that the UK-US Data Access Agreement will come into force on October 3, 2022.

As a reminder, the Data Access Agreement allows the US and the UK law enforcement agencies to directly request data held by communications providers in the other party's jurisdiction in order to prevent, detect, investigate and prosecute serious crimes such as terrorism and child sexual abuse and exploitation.

In October 2019, the UK and US Governments signed an agreement on cross-border law enforcement demands for data from communication service providers. Recently, the two countries have completed the procedural steps required to bring this agreement into force.

For further information: US Department of Justice Website

07/18/2022 – UK Parliament | Regulation | Data Protection and Digital Information Bill

The UK Government published a draft of the Data Protection and Digital Information Bill.

The draft Bill provides for various changes to the UK's legal framework, including replacement of the role of data protection officer with a designated senior responsible individual, changes to record-keeping requirements, replacement of the regime for carrying out data protection impact assessments and removal of the requirement for non-UK organizations to appoint a UK representative, as well as exempting additional types of website cookies from the existing consent requirements.

Please note that the Bill may be subject to substantial change following the announcement in October by the Secretary of State that the UK will be replacing GDPR with a new data protection regime.

For further information: UK Parliament Website

07/05/2022 – UK Government | Data Transfers | Data Adequacy Agreement

The UK and the Republic of Korea reached an adequacy agreement in principle to secure the transfer of data outside of the UK.

For further information: UK Government Website

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)*
- ***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)*
- ***Léna Bionducci** – Associate, Paris (lbionducci@gibsondunn.com)*
- ***Yannick Oberacker** – Associate, Munich (yoberacker@gibsondunn.com)*