GIBSON DUNN

July 8, 2022

GIBSON DUNN | EUROPE | DATA PROTECTION – Q2 2022

To Our Clients and Friends:

Personal Data | Cybersecurity | Technology | Digital

Europe

07/05/2022 – European Union | Regulation | Digital Markets Act | Digital Services Act

The European Parliament held the final vote on the new Digital Services Act (DSA) and Digital Markets Act (DMA), following a deal reached between the Parliament and the Council on 23 April and 24 March respectively.

The DSA sets obligations for digital service providers, such as social media or marketplaces, to tackle the spread of illegal content, online disinformation and other societal risks. These requirements aim to be proportionate to the size and risks platforms pose to society, and their violations can be sanctioned by a fine of up to 6% of the worldwide turnover.

The DMA sets obligations for large online platforms acting as "gatekeepers" (platforms whose dominant online position make them hard for consumers to avoid). DMA requirements include allowing third parties to inter-operate with a gatekeeper's own services, a prohibition to rank its own services or products more favorably, and an obligation to collect consent to process users' personal data for targeted advertising. Fines will be up 10% of the gatekeeper's total worldwide turnover, or up to 20% in case of repeated non-compliance.

Once formally adopted by the Council in July (DMA) and September (DSA), both Acts will be published in the EU Official Journal and enter into force twenty days after publication. The DSA will apply fifteen months or from January 1, 2024 (whichever comes later) after the entry into force (or, for very large providers, four months after they have been designated as such by the Commission). The DMA will apply six months following its entry into force, and the gatekeepers will have a maximum of six months after they have been designated as such to comply with the new obligations.

For further information: European Parliament Website; DMA Client Alert

06/22/2022 – Court of Justice of the European Union | Decision | Data Protection Officer

The Court ruled that national legislation can impose stricter requirements than the GDPR as regards termination of a Data Protection Officer's (DPO) employment contract, so long as it is compatible with the objectives of the GDPR.

In this case, the Court held as valid provisions of German law prohibiting the termination of a DPO's employment contract without a proper cause, even if the contractual termination is not related to the performance of that DPO tasks. Here, the employer invoked the outsourcing of the data protection service.

For further information: CJEU Website

06/16/2022 – European Data Protection Board | Guidelines | Certification as a Tool for Transfers

The European Data Protection Board adopted Guidelines on certification as a tool for transfers.

As the GDPR introduces certification as a new tool to transfer personal data to third countries in the absence of an adequacy agreement, these Guidelines aim to provide further clarification on the practical use of this transfer tool. The Guidelines focus on certain aspects of certification such as purpose, scope, actors involved, and criteria for demonstrating the existence of appropriate safeguards for transfers. They will be subject to public consultation until the end of September.

For further information: EDPB Website

05/30/2022 – European Union | Regulation | Data Governance Act

The EU published the Data Governance Act, which creates a framework for data sharing and is due to apply from September 24, 2023.

The Regulation aims at encouraging the reuse of data held by public sector bodies. The Regulation provides for the creation of data intermediaries to act as brokers between data providers and data users and encourages data altruism (non-profit-based data sharing activity). The Data Governance Act also creates a European Data Innovation Board tasked with advising the Commission on data governance.

For further information: EU Website

05/25/2022 – European Commission | Questions and Answers | Standard Contractual Clauses

The European Commission published a Q&A on the set of Standard Contractual Clauses issued on June 4, 2021.

The purpose of this Q&A is to provide practical guidance on the use of the Standard Contractual Clauses to assist stakeholders with their compliance efforts. The content of the document will be updated as new questions arise.

For further information: European Commission Website

05/16/2022 – European Data Protection Board | Guidelines | Calculation of Fines

The European Data Protection Board published its Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

The Guidelines aim at harmonizing the methodology supervisory authorities use when calculating of the amount of the fine. They provide for a 5-step calculation methodology: (i) establish whether the case at stake concerns one or more instances of sanctionable conduct and if they have led to one or multiple infringements; (ii) rely on a starting point for the calculation of the fine, according to the Board's harmonized method, (iii) consider aggravating/mitigating factors which could increase or decrease the amount of the fine, (iv) determine legal maximum of fines, (v) analyze whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality or whether further adjustments are necessary.

For further information: EDPB Website

05/13/2022 – European Council | Regulation | NIS Directive

The European Council and the European Parliament agreed on measures for a high common level of cybersecurity across the Union, as part of the NIS 2 Directive.

As a reminder, NIS2 will set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that will be covered by the Directive, such as energy, transport, health and digital infrastructure.

For further information: European Council Website

05/12/2022 – European Data Protection Board | Guidelines | Amicable Settlements

The European Data Protection Board published its Guidelines 06/2022 on the practical implementation of amicable settlements, which are often used by supervisory authorities when dealing with complaints.

The Guidelines seek to address inconsistencies in Member States' approach of amicable settlements sought following cross-border complaints. The Guidelines also contains a checklist for handling a case via amicable settlement.

For further information: EDPB Website

05/11/2022 – European Commission | Proposal for a Regulation | Child Sexual Abuse

The European Commission issued a Proposal for a Regulation laying down rules to prevent and combat child sexual abuse.

The current version of the Proposal requires that certain technical providers install and operate technologies detecting the dissemination of child abuse material or solicitation of children. Penalties will be defined by Member States and capped at 6% of the annual income or global turnover of the preceding business year of the provider.

For further information: European Commission Website

05/04/2022 – European Data Protection Board | Joint Opinion | Data Act

The European Data Protection Board and the European Data Protection Supervisor issued a Joint Opinion on the Proposal for a Data Act.

Both Authorities noted that highly sensitive data could be revealed through sharing mechanisms and that additional safeguards are required to ensure that data sharing does not lower the protection of individuals' right to privacy. The Authorities pointed out some inconsistencies in the Data Act when viewed in relation to other regulations and expressed concern that the supervision mechanism provided for by the Act will lead to fragmented and incoherent supervision.

For further information: EDPB Website

05/02/2022 – European Commission | Proposal for a Regulation | European Health Data Space

The European Commission issued a Proposal for a Regulation on the European Health Data Space establishing a health-specific data sharing framework.

For further information: European Commission Website

04/28/2022 – European Data Protection Board | Statement | Enforcement Cooperation

The European Data Protection Board issued a statement on enforcement cooperation between supervisory authorities to allow for a more consistent application of the GDPR.

According to this statement, supervisory authorities will collectively identify cross border cases of strategic importance for which cooperation will be prioritized. Among other measures, the Board will issue a template for data subjects' complaints and identify best practices regarding the interpretation of national procedural law to ensure a more effective application of the GDPR.

For further information: EDPB Website

04/12/2022 – European Data Protection Supervisor | Reprimand | Migration to the Cloud

The European Data Protection Supervisor issued a Reprimand to the European Border and Coast Guard Agency (Frontex) for moving to the cloud without conducting a proper data protection impact assessment.

According to the Supervisor, Frontex moved to the cloud without a timely, exhaustive assessment of the data protection risks and without the identification of appropriate mitigating measures or relevant safeguards for processing. Frontex also failed to demonstrate the necessity of the planned cloud services and compliance with data minimization requirements.

For further information: EDPS Website

04/07/2022 – European Data Protection Board | Statement | Data Transfers

The European Data Protection Board adopted a statement on the new Trans-Atlantic Data Privacy Framework.

The Board welcomes the commitments made by the US to take "unprecedented" measures to protect the privacy and personal data of individuals in the EU when their data are transferred to the US. That said,

it highlights that this political agreement has not been translated into concrete legal proposals yet, and that it will assess carefully the improvements that the new framework may bring.

For further information: EDPB Website

Austria

04/22/2022 – Austrian Supervisory Authority | Decision | Google Analytics

The Austrian Supervisory Authority issued a decision against a company using Google Analytics, reaffirming that the tool cannot be used in accordance with the GDPR.

In particular, the Authority holds that the GDPR does not recognize a risk-based approach. Accordingly, the fact that US intelligence services have no interest in the data processed does not matter in assessing the effectiveness of the measures. In this case, no fine was issued against the controller as the use of Google Analytics had ceased before the procedure was finalized.

For further information: DSB Decision [DE]

France

06/30/2022 – French Supervisory Authority | Sanction | Commercial Prospecting

The French Supervisory Authority fined an energy company €1 million for failure to respect data subject rights.

According to the decision, the company failed to allow individuals to object to commercial prospecting, as one of its subscription form provided no means to object to the re-use of data for the purposes of commercial canvassing for similar products or services. In addition, the company failed to comply with its obligation to inform data subjects, as well as with access and objection rights.

For further information: CNIL Website

06/07/2022 – French Supervisory Authority | Guidance | Google Analytics

The French Supervisory Authority issued formal notices against companies using Google Analytics, requiring them to bring the related transfers of personal data to the US in compliance with the GDPR or, if needed, to stop using the tool within a month.

Later, the Authority published guidance on how to use Google Analytics' in a compliant manner, as well as a Q&A on the same topic.

The guidance clarifies that the sole modification of Google Analytics' settings, or the encryption of generated identifiers, is not enough to satisfy the requirements of the Schrems II ruling, in particular since it does not prevent transfers to the US nor re-identification of data subjects. The Authority assesses that a solution could be the use of a proxy in order to avoid any direct contact between individuals' terminal and Google servers, provided that certain requirements are met.

For further information: CNIL Website; Decision; Guidance [FR]; Q&A [FR]

05/16/2022 – French Supervisory Authority | Guidance | Cookie Walls

The French Supervisory Authority published its first criteria to assess the lawfulness of cookie walls.

The Authority advises to provide users who refuse cookies with a fair and equal alternative to access the website without allowing the processing of their data. Monetary compensation is not illegal but should be set at a reasonable amount. When users choose to pay, only necessary cookies may be placed.

For further information: CNIL Website [FR]

04/15/2022 – French Supervisory Authority | Sanction | Data Breach

The French Supervisory Authority imposed a €1.5 million fine on a processor, a French company selling software solutions for medical analysis laboratories, following a data breach concerning 500,000 individuals.

As a result of security weaknesses, medical information (including regarding HIV, cancers, genetic diseases, pregnancies, drug therapy of patients, or genetic data) of individuals was released on the Internet. At the time of the breach, the Supervisory Authority referred the matter to the Paris judicial court, which blocked access to the website on which the leaked data was published.

The fine is imposed on the company acting as processor, for (i) acting beyond the instruction given by the controllers, (ii) breach of the obligation to ensure the security of the processing, and (iii) failure to implement the contractual measures required pursuant to Article 28(3) of the GDPR.

For further information: CNIL Decision [FR]

04/07/2022 – French Supervisory Authority | Formal Notice | Marketing

The French Supervisory Authority issued formal notices to three companies for sharing personal data of clients and prospects to their partners without informing data subjects nor collecting their consent.

The companies' partners used the personal data to conduct email and text marketing purposes. Pursuant to the formal notices, the companies had three months to comply with regulations.

For further information: CNIL Website [FR]

04/05/2022 – French Supervisory Authority | Artificial Intelligence | Self-Evaluation | Best Practices

The French Supervisory Authority issued guidance for organization to conduct self-evaluations of their AI-systems in light of the GDPR, as well as best practices when creating and operating AI technologies.

The Authority notably addresses issues related to training data, algorithm development, data processing security, and data subject rights.

For further information: Guidance [FR]; Check-list [FR]

04/12/2022 – French Supervisory Authority | Guidance | Sanction Procedure

Following new legislation on the same topic, the French Supervisory Authority issued guidance on its simplified sanction procedure.

As a reminder, subject to certain conditions, the president of the Authority may now decide alone to issue (i) a warning, (ii) an injunction to comply with the GDPR with a daily penalty of up to €100, and (iii) an administrative fine up to €20,000.

For further information: CNIL Website [FR]

Germany

06/23/2022 – Federal Office for Information Security | Guidance | Healthcare Applications

The Federal Office for Information Security issued guidance to assist developers of applications that process or store sensitive data to create secure solutions.

The guidance defines security levels and a security risk assessment for mobile and web applications, as well as for background systems. In addition, the guidance provides for specific security requirements for healthcare applications with biometric user authentication. In particular, the use of biometric authentication methods will only be permitted for devices contained in a white list of suitable devices established by the Authority. All other devices shall not use biometric authentication methods and will have to be limited to the classic PIN/password method.

For further information: BSI website [DE]

06/02/2022 – Niedersachsen Supervisory Authority | Activity Report | On-Premise Inspection

In its activity report, the Niedersachsen Supervisory Authority provided guidelines on how to prepare for on-premise inspections by supervisory authorities.

For further information: Niedersachsen Authority Website [DE]

05/16/2022 – Berlin Supervisory Authority | Guidance | Data Transfers

The Berlin Supervisory Authority issued guidance on cross-border data transfers following the Schrems II ruling.

The Authority outlines the requirements for cross-border data transfers and clarifies the current legal situation regarding international data transfers while examining the US surveillance framework, the Schrems II ruling and their implications. The guidance also states that the Authority is taking part in a cross-state campaign to implement the Schrems II ruling, involving 900 companies. After a preliminary examination, most of them were found to have failed grasping the legal issues arising from Schrems II.

For further information: BInBDI Website [DE]

05/09/2022 – Brandenburg and Hamburg Supervisory Authorities | Cookie Banners

The Brandenburg and Hamburg Supervisory Authorities informed companies, on May 9 and April 4, that the consent banner on their website does not comply with data protection requirements.

The Authorities held that the companies do not allow users to deny their consent as easily as to grant it and affirmed that a "reject all" button should become the standard for cookie banners.

For further information: Brandenburg Authority Website [DE]; HmbBfDI Website [DE]

03/24/2022 – German Data Protection Conference | Resolution | Online Commerce

The German Data Protection Conference (DSK) issued a resolution regarding online commerce and the need for guest account orders.

The DSK held that online purchases must not be made solely available via registered customer accounts, but must also be possible through a guest access that does not require the customer to register with the vendor. In the DSK's view, where purchases are only possible for registered customers, the underlying consent is invalid if the registration was mandatory for the individual to proceed with the purchase.

For further information: DSK Website [DE]

Ireland

06/27/2022 – Irish Supervisory Authority | Prosecution Proceedings | Commercial Prospecting

The Irish Supervisory Authority issued a statement, welcoming the conviction of a telecommunication company in relation to marketing offenses.

The case concerned a customer who received a marketing call, after having opted out of marketing, due to a human error made by the company. The company was sanctioned to donate €500 to a charity.

For further information: DPC Website

Italy

06/23/2022 – Italian Supervisory Authority | Sanction | Google Analytics

The Italian Supervisory Authority banned the use of Google Analytics, due to the lack of adequate safeguards for data transfers to the US. Accordingly, it issued a reprimand against a website operator, to be followed by others.

This decision complements the decisions of other supervisory authorities on Google Analytics. The Authority gave the operator 90 days to bring its activity in compliance with the GDPR.

For further information: Garante Website [IT]

Netherlands

05/06/2022 – Dutch Supervisory Authority | Sanction | Blacklisting

The Dutch Supervisory Authority imposed a €3.7 million fine on its tax administration for illegal processing of personal data in its blacklist, used to register indications of fraud, often with major repercussions for people who had been wrongly included on the list.

The Authority found that the tax administration had no statutory basis for processing the personal data on the list, and failed to comply with the principles of data accuracy and security.

For further information: AP Website

Norway

06/28/2022 – Norwegian Supervisory Authority | Sanction | Data Breach

In January 2022, the Norwegian Supervisory Authority issued a €196.400 fine (NOK 2.000.000) against the Parliament, following a data breach related to employees' email accounts in 2020.

The Authority emphasizes the absence of two-factor authentication or similar effective security measures to achieve adequate protection.

For further information: Datatilsynet Website [NOR]

06/24/2022 – Norwegian Supervisory Authority | Sanction | Identity Verification

The Norwegian Supervisory Authority fined a company €483.000 fine (NOK 5.000.000) for failing to implement adequate security measures, this allowing its members to access other individuals' shopping history.

The Authority also clarifies that such unauthorized access constitutes a data breach.

For further information: Datatilsynet Website [NOR]

06/14/2022 – Norwegian Supervisory Authority | Decision | Legal Basis

The Norwegian Supervisory Authority issued a decision against a company using a browser extension to identify individuals as trans-friendly or transophobic, and imposed a ban on the use of this tool on Norwegian territory.

The Authority found that such processing had no legal basis, and that the controller failed to comply with transparency requirements as well as data subject rights.

For further information: Datatilsynet Website

04/04/2022 – Norwegian Supervisory Authority | Guidance | Children Personal Data

The Norwegian Supervisory Authority issued guidance on the sharing of children's data and consent.

The Authority highlights that specific rules exist regarding children, especially in the areas of social media, health, education, associations and religious or philosophical communities, as well as e-commerce.

For further information: Datatilsynet Website [NOR]

Spain

05/18/2022 – Spanish Supervisory Authority | Sanction | Third-Party Data Transfer

The Spanish Supervisory Authority fined a US-based company €10 million for transferring data to third parties without legal basis and for failure to comply with data subjects' rights.

The fine concerns processing conducted in the framework of the Lumen Project, a US-based academic project collecting and studying legal requests for removal of online information. The Authority also ordered the company to bring its processing in compliance, and to delete all personal data that has been subject to a request for erasure and then communicated to the Lumen Project (including by ordering the Lumen Project to do the same).

For further information: AEPD Website [ES]

05/03/2022 – Spanish Data Supervisory Authority | Guidance | Health Data

The Spanish Supervisory Authority issued guidance regarding processing of health data.

The guidance focuses on data subjects' rights in relation to health data, processing for health research and clinical trials and personal data breaches in the healthcare sector.

For further information: AEPD Website [ES]

United Kingdom

06/23/2022 – UK Government | Data Strategy | Proposals

The UK Government issued its response to the consultation on its reform of the UK's data protection laws.

The Government's ambition is to establish the UK as the most attractive global data marketplace, and it intends to depart from the GDPR in certain areas. For example, the reform aims at easing the use of automated decision-making, clarifying the threshold for anonymization, replacing the requirement to carry out data protection impact assessments with a new privacy management programme and removing the requirements for data protection officers (replaced with an individual responsible for the privacy management programme).

The Government also contemplates changes to the Privacy and Electronic Communications Regulations, removing the requirement for consent in relation to certain types of website cookies and increasing the maximum fine for violation of the Regulations to £17.5 million or 4% of a business's global turnover.

For further information: ICO Website

05/23/2022 – UK Supervisory Authority | Sanction | Facial Recognition

The UK Supervisory Authority (ICO) issued a fine of over £7.5 million to an American facial recognition company for processing images of people in the UK, collected from publicly available sources.

The ICO found that the company's data processing was subject to the UK GDPR, and that the company failed to provide adequate information to data subjects and did not meet the data protection standards for biometric data, and also found that the data processing lacked a legal basis and a clear data retention policy. Aside from a fine, the ICO also ordered the company to stop obtaining and processing publicly available personal data of UK residents and to delete all UK residents' data from its systems.

For further information: ICO Website

05/10/2022 – UK Supervisory Authority | Toolkit | AI and Data Protection

The UK Supervisory Authority published an AI and Data Protection Toolkit to provide further practical support to organizations to reduce the risks to individuals' rights and freedoms caused by AI systems.

The tool provides a way to assess the risks to fundamental rights and freedoms of individuals and can complement any data protection impact assessment. The Authority provides for risks to be assessed "high", "medium", "low" or "non-applicable".

For further information: ICO 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)*
- ***James A. Cox** – Partner, London (jacox@gibsondunn.com)*
- ***Patrick Doris** - Partner, London (pdoris@gibsondunn.com)*
- ***Kai Gesing** – Partner, Munich (kgesing@gibsondunn.com)*
- ***Joel Harrison** – Partner, London (jharrison@gibsondunn.com)*
- ***Vera Lukic** – Partner, Paris (vlukic@gibsondunn.com)*
- ***Penny Madden** – Partner, London (pmadden@gibsondunn.com)*
- ***Michael Walther** – Partner, Munich (mwalther@gibsondunn.com)*
- ***Sarah Wazen** – Of counsel, London (swazen@gibsondunn.com)*
- ***Léna Bionducci** – Associate, Paris (lbionducci@gibsondunn.com)*
- ***Yannick Oberacker** – Associate, Munich (yoberacker@gibsondunn.com)*
- ***Clémence Pugnet** – Associate, Paris (cpugnet@gibsondunn.com)*

© 2022 Gibson, Dunn & Crutcher LLP

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