

## GIBSON DUNN PARIS | DATA PROTECTION – DECEMBER 2020

To Our Clients and Friends:

### Personal Data Watch

#### Europe

11/27/2020 – [Committee of Convention 108 | Guidelines | Children's data protection in education setting](#)

**The Council of Europe's Committee of Convention 108 published guidelines on children's data protection in an education setting.**

For further information: [Council of the Europe Website](#)

---

11/20/2020 – [Presidency of the Council of the European Union | Progress report | ePrivacy Regulation](#)

**The European Data Protection Board (EDPB) published a statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB.**

In particular, the EDPB expressed its concerns about the latest developments regarding the enforcement of the future ePrivacy Regulation, which would create fragmentation of supervision, procedural complexity, as well as lack of consistency and legal certainty.

For further information: [EDPB Website](#)

---

11/17/2020 – [European Data Protection Supervisor | Opinion | European Health Data Space](#)

**The European Data Protection Supervisor published a Preliminary Opinion on the European Health Data Space, which aims to highlight the essential elements to be taken into account in its elaboration from a data protection perspective.**

For further information: [EDPB Website](#)

---

11/10/2020 – [European Data Protection Board | Document | Procedure for the development of informal Codes of Conduct sessions](#)

**The European Data Protection Board (EDPB) published a document on the procedure for the development of informal “Codes of Conduct sessions”.**

For further information: [EDPB Website](#)

---

11/12/2020 – [European Commission | Draft Standard Contractual Clauses](#)

**The European Commission published two draft Standard Contractual Clauses: (i) the first to carry out an international transfer of data to a third country in the absence of an adequacy decision under Article 46 of the GDPR, and (ii) the second to regulate the relationship between data controller and data processor in accordance with the requirements of Article 28.**

The draft Standard Contractual Clauses for data transfers to a third country addresses four different transfer scenarios (controller to controller; controller to processor, but now also processor to processor and processor to controller), and also addresses the issue of access by third country governments to the transferred data. It should be noted that the draft provides for a transitional period of one year from the entry into force of the new clauses, during which it will be possible to continue to use the old clauses for the performance of a contract concluded before that date. Once finalized, businesses should therefore factor in the foreseeable need to put all previous data transfer relationships on a new contractual basis within the year of 2021.

In addition, the Commission has published a draft standard contractual clauses between controllers and processors. This model is intended to help businesses to comply with the requirements of Article 28 of the GDPR, but is not mandatory. Organizations will therefore be able to continue to use their own processing agreements. Both projects are open for public consultation until December 10.

For further information: [Draft Standard Contractual Clauses](#) ; [Draft Data Processing Agreement](#)

---

11/11/2020 – [Court of Justice of the European Union | Ruling | Consent](#)

**The Court of Justice of the European Union, in its ruling *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*, decided that a contract for the provision of telecommunications services containing a clause stating that the customer has consented to the collection and storage of his or her identity document cannot demonstrate that that customer has validly given his or her consent where the box referring to that clause has been ticked by the data controller before the contract was signed.**

The Court specifies that this is also the case where the customer is misled as to the possibility of concluding the contract if he or she refuses to consent to the processing of his or her data, or where the freedom to choose to object to that collection and storage is affected by the requirement to complete an additional form setting out that refusal.

For further information: [CJEU Website](#)

---

11/10/2020 – [European Data Protection Board | Recommendations | Data transfers](#)

**The European Data Protection Board (EDPB) adopted recommendations on "supplementary measures" that supplement transfer tools to ensure compliance with the EU level of protection of personal data.**

The EDPB recommends that data exporters (i) map all transfers of personal data to third countries and verify that the data transferred are adequate, relevant and limited to what is necessary; (ii) verify the transfer tool on which the transfers are based; (iii) assess whether there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards, and document this assessment; (iv) identify and adopt additional measures (examples are provided in Annex 2 of the Recommendations); (v) take any formal procedural steps that the adoption of the supplementary measure may require; and (vi) re-evaluate at appropriate intervals the level of protection afforded to the data transferred.

The recommendations are open for public consultation, which have been extended from 30 November 2020 until 21 December 2020, but are nevertheless applicable as soon as they are published.

For further information: [EDPB Website](#) ; [EDPB Infographic](#)

---

11/09/2020 – [European Data Protection Board | Decision | Article 65 dispute resolution procedure](#)

**The European Data Protection Board (EDPB) adopted its first decision under the dispute resolution mechanism of Article 65 of the GDPR.**

The EDPB adopted its binding decision two months after the opening of the Article 65 procedure, the default deadline of one month having been extended by a further month due to the complexity of the matter.

Finally, the EDPB published a FAQ on Article 65 of the GDPR, which deals, inter alia, with the possibilities to challenge a decision of the EDPB taken on this basis.

For further information: [EDPB Website](#)

---

11/03/2020 – [Council of the Europe](#) | [Ratification](#) | [Convention 108+](#)

**The Council of the Europe announced that Malta had ratified Convention 108+. Malta is the ninth country to ratify Convention 108+.**

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

---

## Belgium

11/17/2020 – [Belgian Supervisory Authority](#) | [Toolbox](#) | [Tools to help with the implementation of the GDPR](#)

**The Belgian Data Protection Authority provided tools to assist organizations with the implementation of the GDPR.**

For further information: [APD Website](#)

---

## Denmark

12/01/2020 – [Danish Supervisory Authority](#) | [Guidelines](#) | [Data protection in employment relationships](#)

**The Danish Supervisory Authority issued revised guidelines on data protection in the employment relationship context, following discussions with representatives of the social partners about union representatives' use of the employer's IT equipment.**

For further information: [Datatilsynet Website](#)

---

11/25/2020 – [Danish Supervisory Authority](#) | [Guidance](#) | [Recording telephone conversations](#)

**The Danish Supervisory Authority issued its guidance on recording telephone conversations for documentation and training purposes.**

For further information: [Datatilsynet Website](#)

---

## France

12/10/2020 – [French Supervisory Authority](#) | [Sanction](#) | [ePrivacy](#) | [Cookies](#)

**The French Supervisory Authority (CNIL) fined Google LLC 60 million euros and Google Ireland Limited 40 million euros, as well as, under another decision, Amazon Europe Core 35 million euros, for allegedly “having placed advertising cookies on user’s computers without obtaining prior consent and without providing adequate information”.**

According to the CNIL, when a user visited the websites google.fr and amazon.fr, several cookies used for advertising purposes were automatically placed, without any action on the user’s part. The CNIL also claims that the information provided was neither clear, nor complete.

To set the amount of the fine, the CNIL took into account, inter alia, the seriousness of the breaches, the importance of personalized ads for the companies’ businesses, as well as the millions of French users impacted. In addition to the financial penalty, the companies are also ordered to remedy the ongoing breaches, under a €100,000 additional penalty for each day of delay.

Regarding the jurisdiction, the CNIL ruled being both (i) materially competent as it considers the one-stop shop mechanism as not applicable in procedures relating to the use of cookies that fall under the "ePrivacy" directive; and (ii) territorially competent because the use of cookies would be carried out within the framework of the activities of the companies concerned.

These are the highest penalties ever imposed under data protection regulations.

For further information: [CNIL's summary of the Google Decision](#) ; [CNIL's summary of the Amazon Decision](#)

---

11/30/2020 – [French Supervisory Authority](#) | [Statement](#) | [Government SMS messages](#)

**The French Supervisory Authority issued a statement confirming the legality of the SMS messages received from the government regarding the TousAntiCovid app in the context of the reopening of shops in France.**

For further information: [CNIL Website](#)

---

11/12/2020 – [French Supervisory Authority](#) | [Q&A](#) | [Remote working](#)

**The French Supervisory Authority (CNIL) published questions and answers on remote working.**

In particular, the CNIL points out that the employer must inform all employees, prior to their implementation, of any measures designed to control their activity. Moreover, processing operations for

monitoring the activity of employees must be included in the register of processing activities and must be subject to an impact assessment in exceptional cases where constant monitoring is possible.

For further information: [CNIL Website](#)

---

## Germany

11/25/2020 – [German Data Protection Conference | Resolution | Criticism about implementation of the ePrivacy Directive in Germany](#)

**The German Data Protection Conference (DSK) has adopted a resolution criticizing the German legislator for not fully and not correctly implementing the ePrivacy Directive into German law.**

The DSK pointed out that website operators need legal certainty with regard to the use of tracking cookies. According to the DSK, the “Planet49” decision of the German Federal Court of Justice (decision of May 28, 2020 – I ZR 7/16) has highlighted the need for the legislator to amend the existing rules contained in the German Telemedia Act, which implements the ePrivacy Directive into German law. In the DSK’s view, the German Telemedia Act is not in line with the provisions of the GDPR when it comes to the “opt-in principle” with regard to the processing of personal data.

For further information (in German): [DSK Website](#)

---

11/20/2020 – [Baden-Württemberg Supervisory Authority | Statement | Supplementary measures](#)

**The Baden-Württemberg Supervisory Authority published a statement on the supplementary measures proposed by a major U.S. company to comply with the Schrems II decision.**

These supplementary measures will be assessed by the competent authorities, in particular by the Federal Conference of German Supervisory Authorities (DSK) and the federal authorities of Baden-Württemberg, Bavaria and Hesse – and this review is likely to result in additional guidance for businesses.

For further information: [LfDI Baden-Württemberg Website](#)

---

11/11/2020 – [Regional Court of Bonn | Decision | Fine Reduced](#)

**The Regional Court of Bonn ruled on a fine that was imposed on a German telecommunications company in 2019 for alleged insufficient user authentication measures and safeguards in a call center.**

While the court confirmed the violation of the GDPR, the court significantly reduced the fine from € 9.55 million to €900,000.

---

11/06/2020 – [Rhineland-Palatinate Supervisory Authority | Warning | Excessive health information requests](#)

**The Rhineland-Palatinate Supervisory Authority issued a warning against a school administration for requesting excessive data regarding the medical certificates of persons exempted from wearing masks during the COVID-19 pandemic.**

For further information: [Rhineland-Palatinate Supervisory Authority Website](#)

---

11/03/2020 – [Rhineland-Palatinate Supervisory Authority | Transfers | Checklist](#)

**The Rhineland-Palatinate Supervisory Authority published a checklist on data transfers to third countries. The DPA's flow chart illustrates the implications of the Schrems II decision (German language).**

For further information: [Rhineland-Palatinate Supervisory Authority Website](#)

---

## Italy

11/16/2020 – [Italian Supervisory Authority | Sanction | Telemarketing, acquisition of contact lists and security measures](#)

**The Italian Supervisory Authority (Garante) fined a telephone operator more than 12 million euros for failing to obtain the data subjects' consent and insufficient security measures.**

In addition to the fine, the Garante ordered the company to bring its telemarketing processing in compliance with consent requirements, to strengthen its security measures so as to prevent unauthorized access to customer databases and to respond to requests for the exercise of rights made by certain users.

For further information: [Garante Website](#)

---

## Luxembourg

11/26/2020 – [Luxembourgish Supervisory Authority | 2019 Annual Report](#)

**The Luxembourgish Supervisory Authority (CNPD) issued its 2019 Annual Report.**

For further information: [CNPD Website](#)

---

## Netherlands

11/26/2020 – [Dutch Supervisory Authority | Violations | Employee temperature measurements](#)

**The Dutch Supervisory Authority (AP) found that two companies measuring staff body temperature during the Coronavirus pandemic violated the GDPR.**

The AP noted that although explicit consent may, in many cases, allow for the processing of special category data, consent is not sufficient in the employment context.

For further information: [AP Website](#)

---

## Spain

11/20/2020 – [Spanish Supervisory Authority | Guidance | Blockchain](#)

**The Spanish Supervisory Authority published guidance on the basic concepts of blockchain in relation to data protection.**

For further information: [AEPD Website](#)

---

11/16/2020 – [Spanish Supervisory Authority | Sanction | Legal basis](#)

**The Spanish Supervisory Authority fined a telecommunications operator €36,000 for processing data without a legal basis, in the absence of a contract with the data subject.**

For further information: [AEPD Website](#)

---

11/04/2020 – [Spanish Supervisory Authority | Statement | Zero-knowledge proofs](#)

**The Spanish Supervisory Authority published a statement on zero-knowledge proofs.**

Zero-knowledge proofs are a set of techniques that can be used to demonstrate that certain information is accurate without disclosing it, thus facilitating the implementation of the data minimization principle.

For further information: [AEPD Website](#)

---

10/29/2020 – [Spanish Supervisory Authority | Sanction | Failure to appoint a data protection officer](#)

**The Spanish Supervisory Authority fined a company €50,000 for failing to comply with its obligation to appoint a data protection officer.**

As a result, a data subject had not been able to exercise his or her rights relating to data processing linked to a video surveillance system implemented by the company.

For further information: [AEPD Website](#)

---

## Sweden

11/26/2020 – [Swedish Supervisory Authority | Investigations | Data transfers](#)

**The Swedish Supervisory Authority announced that it had initiated six investigations related to international data transfers following complaints made by the association NOYB.**

For further information: [Datainspektionen Website](#)

---

11/24/2020 – [Swedish Supervisory Authority | Sanction | Data Breaches](#)

**The Swedish Supervisory Authority fined a Board of Education SEK 4 million (approx. €393,610) for lack of security in its IT system leading to several data breaches.**

In its decision, the Swedish Data Protection Authority finds that the Board of Education had failed to take adequate technical and organizational measures to ensure a level of security appropriate to the risk, including a procedure for regularly testing, examining and evaluating the effectiveness of the technical security measures.

For further information: [Datainspektionen Website](#)

## United Kingdom

11/13/2020 – [UK Supervisory Authority](#) | [Sanction](#) | [Failure to comply with the security obligation](#)

**The UK Supervisory Authority fined a company selling concert tickets to £1.25 million for failing to comply with its security obligations, in the context of a cyber-attack on a chat-bot installed on its online payment page.**

The data breach potentially affected the data of 9.4 million people.

For further information: [ICO Website](#)

---

11/05/2020 – [UK Supervisory Authority](#) | [Guide](#) | [Data relating to criminal offences](#)

**The UK Supervisory Authority published a guide on criminal offence data.**

For further information: [ICO Website](#)

---

## Others

11/12/2020 – [NOYB](#) | [Complaint](#) | [Data breach relating to Maltese voters](#)

**The Association None of Your Business (NOYB) filed a complaint regarding a data breach impacting 337,384 Maltese citizens. The data included a numerical identifier indicating the political opinion of each citizen and was publicly available on Internet.**

For further information: [NOYB Website](#)

---

11/05/2020 – [Open Rights Group](#) | [Complaint](#)

**The Association Open Rights Group is suing the UK Supervisory Authority for its inaction regarding illegal practices of the Adtech industry.**

For further information: [Open Rights Group 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))

**James A. Cox** – Partner, London ([jacox@gibsondunn.com](mailto:jacox@gibsondunn.com))

**Patrick Doris** - Partner, London ([pdoris@gibsondunn.com](mailto:pdoris@gibsondunn.com))

**Penny Madden** – Partner, London ([pmadden@gibsondunn.com](mailto:pmadden@gibsondunn.com))

**Michael Walther** – Partner, Munich ([mwalther@gibsondunn.com](mailto:mwalther@gibsondunn.com))

**Kai Gesing** – Of counsel, Munich ([kgesing@gibsondunn.com](mailto:kgesing@gibsondunn.com))

**Alejandro Guerrero** – Of counsel, Brussels ([aguerrero@gibsondunn.com](mailto:aguerrero@gibsondunn.com))

**Vera Lukic** – Of counsel, Paris ([vlukic@gibsondunn.com](mailto:vlukic@gibsondunn.com))

**Sarah Wazen** – Of counsel, London ([swazen@gibsondunn.com](mailto:swazen@gibsondunn.com))

**Adélaïde Cassanet** – Associate, Paris ([acassanet@gibsondunn.com](mailto:acassanet@gibsondunn.com))

**Franziska Gruber** – Associate, Munich ([fgruber@gibsondunn.com](mailto:fgruber@gibsondunn.com))

**Selina Grün** – Associate, Munich ([sgruen@gibsondunn.com](mailto:sgruen@gibsondunn.com))

**Clémence Pugnet** – Associate, Paris ([cpugnet@gibsondunn.com](mailto:cpugnet@gibsondunn.com))

© 2020 Gibson, Dunn & Crutcher LLP

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