

## GIBSON DUNN PARIS | DATA PROTECTION – NOVEMBER 2020

To Our Clients and Friends:

### Personal Data Watch

#### Europe

10/29/2020 – [European Data Protection Supervisor | Strategy | Schrems II ruling](#)

**The European Data Protection Supervisor (EDPS) published its Strategy for Union institutions, offices, bodies and agencies (EUIs) to comply with the Schrems II Ruling.**

As a short-term compliance action, the EDPS reminds that it has issued an order to EUIs for them to complete a mapping exercise identifying transfers of data currently carried out, and strongly encourages EUIs to avoid new processing activities that involve transfers of personal data to the United States.

As a medium-term compliance action, EUIs will be asked to carry out case-by-case Transfer Impact Assessments (TIAs) to identify, for the specific transfer at stake, whether an essentially equivalent level of protection is afforded in the third country of destination, and, depending on the results of such TIAs, to report to the EDPS.

Finally, the EDPS specifies that it will start exploring the possibility of joint assessments, carried out with the other data protection authorities, of the level of protection of personal data afforded in third countries in order to provide guidance to controllers.

For further information: [EDPS Website](#)

---

10/26/2020 – [Court of Justice of the European Union | Request for a preliminary ruling | Proceedings before the civil courts for breaches of the GDPR](#)

**The Court of Justice of the European Union announced that it has received a request for a preliminary ruling from a German court.**

The question is whether the GDPR precludes national rules which empower competitors, associations, entities and chambers to bring proceedings before the civil courts for breaches of GDPR, independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions.

For further information: [Court of Justice Website](#)

---

10/20/2020 – [European Data Protection Board | Guidelines | Data Protection by Design and by Default](#)

**The European Data Protection Board (EDPB) adopted the final version of its Guidelines on Data Protection by Design and by Default after public consultation.**

For further information: [EDPB Website](#)

---

10/19/2020 – [European Commission | Launch | Interoperability gateway service for national contact tracing](#)

**To exploit the full potential of contact tracing apps to break the chain of COVID-19 across borders, the European Commission announced that its interoperability gateway service linking national apps across the EU is now operational.**

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

---

10/12/2020 – [European Data Protection Board | Guidelines | Concept of relevant and reasoned objection](#)

**The European Data Protection Board (EDPB) published guidelines to establish a common understanding of the concept of "relevant and reasoned" objection of Article 60 of the GDPR.**

As a reminder, under the cooperation mechanism, the Lead Supervisory Authority (LSA) is required to submit a draft decision to the concerned authorities, which can then raise a relevant and reasoned objection within a specific time limit.

If the LSA does not follow the relevant and reasoned objection or if it considers that the objection is not reasoned or relevant, it shall submit the matter to the EDPS in accordance with Article 65 of the GDPR. If the LSA, on the contrary, follows the objection and issues the revised draft decision, the concerned authorities may express a relevant and reasoned objection on the revised draft decision within two weeks.

For further information: [EDPB Website](#)

---

## Belgium

10/01/2020 – [Belgian Supervisory Authority | FAQ | Compliance of small and medium-sized enterprises](#)

**The Belgian Supervisory Authority (APD) published an FAQ regarding compliance of small and medium-sized enterprises with the GDPR.**

For further information: [APD Website](#)

---

09/30/2020 – [Belgian Supervisory Authority | Annual Report](#)

**The Belgian Supervisory Authority (APD) published its 2019 Annual Report.**

In particular, the report indicates that the year was marked by the appointment of its Executive Committee, the first fines taken on the basis of the GDPR and the implementation of its 2020-2025 strategic plan.

For further information: [APD Website](#)

---

## Cyprus

10/19/2020 – [Cypriot Supervisory Authority | Sanction | Data breach](#)

**The Cypriot Supervisory Authority fined a Bank €15,000 for losing the complainant's insurance policy, and failing to notify the related data breach within 72 hours from the moment the loss was brought to its knowledge.**

For further information: [Cypriot Supervisory Authority Website](#)

---

## France

10/28/2020 – [French Supervisory Authority | Guidance | Erasure of data of deceased persons](#)

**The French Supervisory Authority (CNIL) issued guidance on the erasure of personal data of deceased persons with regards to social network accounts.**

The Authority notes that, while the social network accounts are strictly personal and subject to correspondence secrecy, heirs are able to, after proving their identity, ask the data controller to take into account the death of their relatives and to update their account, as well as to request the closure of the

account in the absence of instructions to the contrary by the deceased person. The CNIL also provides a link to the related forms available on the main social networks.

For further information: [CNIL Website](#)

---

10/23/2020 – [French Supervisory Authority | Statement | TousAntiCovid app](#)

**The French Supervisory Authority (CNIL) addressed the TousAntiCovid app for contact tracing in the context of the COVID-19 pandemic, which replaces the former StopCovid app.**

The Authority highlights that, since no significant changes to the processing of personal data were made compared to the former app, it did not require referral to the CNIL. Nevertheless, the CNIL specifies that it will remain vigilant and will monitor any updates, noting that it maintains the right to carry out inspections and act in the event of significant changes.

For further information: [CNIL Website](#)

---

10/13/2020 – [French Administrative Court | Summary proceedings | Health Data Hub platform](#)

**On September 22, 2020, and again on October 13, 2020, the French Administrative Court (Conseil d'Etat) rejected the summary proceedings filed by several organizations and individuals to denounce the transfer of French healthcare data to the United States as part of the Health Data Hub platform.**

Fearing possible transfers of personal data to the United States, associations and unions have asked the French Administrative Court to suspend the Health Data Hub platform as a matter of urgency. The Council of State notes that personal data hosted in the Netherlands under a contract with Microsoft cannot legally be transferred outside the European Union.

While the risk cannot be totally excluded that the US intelligence services may request access to this data, the Court considers that this does not justify, in the very short term, the suspension of the platform, but requires special precautions to be taken, under the supervision of the French Supervisory Authority.

For further information: [Court Website](#)

---

10/09/2020 – [French Supervisory Authority | Good practices | Facial recognition in airports](#)

**The French Supervisory Authority (CNIL) clarified its position on facial recognition for identity control in airports.**

The French Supervisory Authority recalls that facial recognition is a processing of biometric data, which is particularly sensitive, and underlines the main principles to be respected to implement it (e.g., necessity, proportionality, consent).

For further information: [CNIL Website](#)

---

10/07/2020 – [French Supervisory Authority | Recommendation | SQL injection attack](#)

**The French Supervisory Authority (CNIL) issued its recommendations to prevent the extraction of credit card numbers by SQL injection on an e-commerce site.**

The French Supervisory Authority describes the modus operandi of this type of attack and gives advice on its prevention and response.

For further information: [CNIL Website](#)

---

10/01/2020 – [French Supervisory Authority | Guidelines | Cookies](#)

**The French Supervisory Authority (CNIL) adopted amending guidelines and a recommendation on the use of cookies and other tracking devices.**

The amending guidelines recall the applicable law and were adjusted on September 17, 2020 to draw the consequences of the decision of the French Administrative Court of June 19, 2020. The Authority has also adopted a recommendation which, without being prescriptive, is a practical guide intended to inform the actors using trackers on the concrete modalities of collecting the Internet user's consent.

The Authority has also posted a FAQ online, as well as the results of its public consultation.

For further information: [CNIL Website](#)

---

## Germany

10/23/2020 – [German Federal Commissioner for Data Protection and Freedom of Information | Statement | Intelligence service access to messenger services](#)

**The German Federal Commissioner for Data Protection and Freedom of Information (BfDI) issued a statement criticizing the Federal Government's draft law which would permit intelligence services to monitor messenger services.**

The BfDI outlined several shortcomings in the current draft law, such as a lack of clarity in the scope of information collection and a violation of the constitutional separation requirement between police authorities and intelligence services.

For further information: [BfDI Statement](#)

---

10/23/2020 – [German Data Protection Conference | Guidelines | Video Conference Systems](#)

**The German Data Protection Conference (DSK) published guidelines on the use of video conference systems.**

The DSK guidelines acknowledge the importance of video conferencing systems during a pandemic like Covid19 and outlines data privacy requirements for the use of those systems.

For further information: [DSK Website](#)

---

10/22/2020 – [Rheinland Pfalz Supervisory Authority | Warning | Digital Health Apps](#)

**The Rheinland-Pfalz Supervisory Authority (LfDI Rheinland-Pfalz) released a warning on digital health applications. The authority found “serious data protection deficiencies” in a digital health app.**

For further information: [Rheinland-Pfalz Supervisory Authority Website](#)

---

10/08/2020 – [German Data Protection Conference | Requirements for the accreditation of certification bodies](#)

**The German Data Protection Conference (DSK) published its requirements for the accreditation of certification bodies in accordance with article 43(3) of the GDPR.**

For further information: [DSK Statement](#)

---

## Ireland

10/12/2020 – [ICCL | UK adequacy decision](#)

**The Irish Council for Civil Liberties (ICCL) announced on its website that it has asked the European Commission not to take an adequacy decision regarding the United Kingdom on the**

**grounds that the UK Supervisory Authority would not meet the criterion of an "effectively functioning" Supervisory Authority.**

For further information: [ICCL Website](#)

---

09/28/2020 – [Irish Supervisory Authority | Guidance | Tracking of vehicles by employers](#)

**The Irish Supervisory Authority (DPC) published a guide on the tracking by employers of their employees' professional vehicles.**

In particular, the guide emphasizes that a data protection impact assessment will most likely have to be carried out in order to implement such processing, and refers to good practices in this area, such as limiting the time and/or location of monitoring, as well as the possibility of easily disabling such monitoring.

For further information: [DPC Guidance](#)

---

## Italy

10/26/2020 – [Italian Supervisory Authority | Inspection plan](#)

**The Italian Supervisory Authority (Garante) published its inspection plan for the second semester of 2020.**

The Authority will focus on the processing of personal data carried out in relation to, among other things, whistleblowing management systems, intermediaries for electronic invoicing, the management and recording of telephone calls within call centre services, and food delivery organisations.

For further information: [Garante Website](#)

---

10/23/2020 – [Italian Supervisory Authority | Investigation | Deep fake software](#)

**The Italian Supervisory Authority (Garante) initiated an investigation over the use of an artificial intelligence technology enabling to generate fake images and pictures of women, which were subsequently shared on a instant messaging app.**

The Authority highlighted the risks of serious infringements of dignity and privacy, especially when related to minors.

For further information: [Garante Website](#)

09/17/2020 – [Italian Supervisory Authority](#) | [Sanction](#) | [Data breach](#)

**The Italian Supervisory Authority (Garante) imposed a fine of €20,000 to a clinic for disclosing medical online reports.**

While accessing their medical online reports through smartphone, 39 patients had been able to also access a list of other 74 patients, containing their reports and a list of medical exams.

For further information: [Garante Website](#)

---

09/17/2020 – [Italian Supervisory Authority](#) | [Sanction](#) | [Data breach](#)

**The Italian Supervisory Authority (Garante) imposed a fine of €60,000 on a company for failing to implement sufficient security measures when processing applications for a public competition.**

The sanction specifies that due to an incorrect configuration of the application management platform, the personal data of the candidates was accessible online. The subcontractor, in charge of this platform, was also fined.

For further information: [Garante Website](#)

---

## Liechtenstein

09/17/2020 – [Liechtenstein Supervisory Authority](#) | [Model](#) | [Joint controllership Agreement](#)

**The Liechtenstein Supervisory Authority (DSS) published a model of joint controllership agreement.**

For further information: [DSS Website](#)

---

## Lithuania

09/29/2020 – [Lithuanian Supervisory Authority](#) | [Annual Report](#)

**The Lithuanian Supervisory Authority (VDAI) published its 2019 annual report.**

For further information: [VDAI Website](#)

## Netherlands

10/12/2020 – [Minister of Legal Protection](#) | [Answer to parliamentary questions](#) | [Schrems II](#)

**The Minister of Legal Protection, Sander Dekker, published his answer to parliamentary questions on the level of data protection in the USA and the Schrems II ruling.**

For further information: [Minister Answer](#)

---

10/12/2020 – [Dutch Supervisory Authority](#) | [Report](#) | [Processing](#)

**The Dutch Supervisory Authority (AP) published a report on processing agreements in the private sector.**

For further information: [AP Website](#)

---

## Spain

10/22/2020 – [Spanish Supervisory Authority](#) | [Tool](#) | [Data breach notification](#)

**The Spanish Supervisory Authority (AEPD) released a tool for the notification of data breaches, which assists data controllers in understanding whether they are obliged to notify affected data subjects.**

For further information: [AEPD Website](#)

---

10/16/2020 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Cookies](#)

**The Spanish Supervisory Authority (AEPD) fined an airline €30,000 for failing to provide users with the option to reject cookies and instead requiring them to accept cookies in order to continue browsing.**

For further information: [AEPD Website](#)

---

10/08/2020 – [Spanish Supervisory Authority](#) | [Practical guidance](#) | [Data protection by default](#)

**The Spanish Supervisory Authority (AEPD) published a practical guide for Data Protection Officers to facilitate the implementation of the data protection by default principle.**

For further information: [AEPD Website](#)

---

## Sweden

10/20/2020 – [Swedish Supervisory Authority](#) | [Report](#) | [Complaints under the GDPR](#)

**The Swedish Supervisory Authority (Datainspektionen) published a report on the complaints it had received from individuals since the entry into force of the GDPR.**

The report outlines that about a quarter of complaints under the GDPR relates to data subject rights, with the right to erasure being the most common right addressed in complaints.

For further information: [Datainspektionen Website](#)

---

10/05/2020 – [Swedish Supervisory Authority](#) | [Guidance](#) | [Employment and data protection](#)

**The Swedish Supervisory Authority (Datainspektionen) published a guide on employment and data protection.**

The guide concerns in particular data recorded on recruitment systems, employee monitoring and surveillance, and employee biometric data.

For further information: [Datainspektionen Website](#)

---

## United Kingdom

10/30/2020 – [UK Supervisory Authority](#) | [Sanction](#) | [Data breach](#)

**The UK Supervisory Authority (ICO) fined an hotel chain £18.4million for failing to keep customers' personal data secure.**

As a reminder, the hotel chain estimates that 339 million guest records worldwide were affected following a cyber-attack in 2014. The attack remained undetected until September 2018, by which time the attacked company had been acquired by the hotel chain.

In July 2019, the ICO issued the hotel chain with an intention to fine of £99.2 million.

In order to set the final penalty, the ICO considered representations from the hotel chain, the steps the hotel chain took to mitigate the effects of the incident and the economic impact of COVID-19 on its business.

For further information: [ICO Website](#)

---

10/29/2020 – [UK Supervisory Authority | Sanction | Nuisance calls](#)

**The UK Supervisory Authority (ICO) fined a claims management services company £250,000 for making 15.1 million calls over a six-month period from the start of 2019.**

The ICO received 85 complaints from members of the public about the persistent calls they were receiving multiple times a day. A number noted the aggressive and rude nature of the callers and highlighted the distress it was causing them.

The company was unable to provide evidence of consent for the majority of calls it made. Where it did provide evidence, the consent was found to have not been freely given, specific or informed.

For further information: [ICO Website](#)

---

10/27/2020 – [UK Supervisory Authority | Report | Direct marketing data broking sector](#)

**The UK Supervisory Authority (ICO) published its report on data protection compliance in the direct marketing data broking sector, following a two-year investigation into three companies.**

The Authority indicated that it had issued an enforcement notice against one of the companies, and that it had found significant data protection failures in each of them, regarding, among other things, transparency, profiling, and the use of data for direct marketing purposes.

For further information: [ICO Website](#)

---

10/21/2020 – [UK Supervisory Authority | Guidance | Right of access](#)

**The UK Supervisory Authority (ICO) published guidance on the right of access.**

The guidance is aimed at data protection officers and includes practical examples on the matter.

For further information: [ICO Website](#)

10/16/2020 – [UK Supervisory Authority](#) | [Sanction](#) | [Data breach](#)

**The UK Supervisory Authority (ICO) fined an airline company £20 million for a data breach that occurred in 2018.**

The ICO investigation revealed that the company was processing a significant amount of personal data without adequate security measures in place. In this context, the company was subject to a cyber-attack in 2018, compromising the personal and financial data of more than 400,000 of its customers, which it did not detect for more than two months.

As a reminder, the ICO initially announced its intention to fine the company £183.4 million. Yet, the ICO states that it took into account the company's representations and the economic impact of the COVID-19 pandemic on its operations in setting the final amount of the fine.

For further information: [ICO Website](#)

---

## Others

10/11/2020 – [Governments](#) | [Call on companies](#) | [Encryption](#)

**The governments of several countries (UK, Australia, Canada, India, Japan, New-Zealand and USA) signed an international statement calling on technology companies to ensure that end-to-end encryption does not impede public safety but preserves user privacy and cyber security.**

For further information: [International Statement](#)

---

09/30/2020 – [Standard Contractual Clauses](#) | [Letter to U.S. authorities](#)

**The American Bankers Association announced, along with several industry organizations, that it has sent a letter to the U.S. authorities regarding standard contractual clauses (SCCs).**

The organizations call on the U.S. authorities, on the one hand, to indicate to European regulators that they cannot expect companies to explain the U.S. government's surveillance practices when using SCCs, and, on the other hand, to ask them to refrain from enforcement action until further guidance is provided on the use of SCCs.

For further information: [American Bankers Association 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.*