

GIBSON DUNN PARIS | DATA PROTECTION – OCTOBER 2020

To Our Clients and Friends:

Personal Data Watch

Europe

09/07/2020 – [Council of Europe | Statement | Convention 108+ | Schrems II](#)

The Data Protection Commissioner of the Council of Europe, Jean-Philippe Walter, and the Chair of the Committee of Convention 108, Alessandra Pierucci, called for adherence to the amended Convention 108+ in order to protect crossborder data flows from surveillance activities, following the Schrems II judgment of the Court of Justice of the European Union.

For further information: [Council of Europe's Statement](#)

09/04/2020 – [European Data Protection Board | Guidelines | Taskforce](#)

The European Data Protection Board (EDPB) has adopted new guidelines on the concepts of controller and processor, as well as on the targeting of social media users.

The guidelines are now subject to public consultation.

The EDPB has also announced the creation of two taskforces following the Schrems II ruling, one to deal with the 101 complaints filed by None of Your Business, and the other to provide recommendations on supplementary measures that data exporters and importers can be required to take to ensure adequate protection when transferring data.

For further information: [EDPB Website | Guidelines on the concepts of controller and processor in the GDPR | Guidelines on the targeting of social media users](#)

09/04/2020 – [European Court of Human Rights | Ruling | Rejection](#)

The European Court of Human Rights rejected a petition concerning the hacking operations of a British intelligence agency abroad.

The NGO Privacy International and a group of Internet service providers argued that the hacking operations carried out by a British intelligence agency outside the United Kingdom violated the rights to privacy and freedom of expression. Although the Court rejected the claim on procedural grounds, it noted that hacking activities by governments are "particularly intrusive and safeguards are necessary in this area".

For further information: [European Court of Human Rights Ruling](#)

Czech Republic

09/25/2020 – [Czech Supervisory Authority](#) | [Sanction](#) | [Unsolicited marketing](#)

The Czech Supervisory Authority (UOOU) fined a company CZK 6 million (approx. €221,200) for repeatedly sending marketing messages without obtaining consent.

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

France

09/23/2020 – [French Supervisory Authority](#) | [Covid-19](#)

The French Supervisory Authority (CNIL) has restated certain principles relating to the collection of data concerning employees, agents or visitors.

In particular, the CNIL reminds the good practices regarding temperature checks at the entrance of the premises, performance of serological tests, questionnaires on health, and work reorganization.

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

09/07/2020 – [French Supervisory Authority](#) | [White paper](#) | [Vocal assistants](#)

The French Supervisory Authority (CNIL) has published a white paper on the ethical, technical and legal issues of vocal assistants.

In particular, the CNIL specifies that the voice is a biometric characteristic allowing the identification of an individual. The white paper contains best practices and notably insists on the transparency and security of the devices in order to comply with the GDPR and respect the individuals' privacy.

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

09/04/2020 – [French Supervisory Authority](#) | [Closure of a formal notice](#) | [StopCovid App](#)

The French Supervisory Authority (CNIL) announced the closure of the formal notice against the Ministry of Solidarity and Health regarding the StopCovid App.

In July, the President of the CNIL issued a formal notice requiring the Ministry to bring the StopCovid App into compliance within one month. According to the authority, the responses provided by the Ministry in August demonstrated that the shortcomings identified during the audit had ceased. The Ministry has taken the necessary steps to comply with the injunctions of the formal notice.

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

09/02/2020 – [French Supervisory Authority](#) | [Best practices](#) | [Elasticsearch](#)

The French Supervisory Authority (CNIL) has published 4 best practices relating to the use of the Elasticsearch search and analysis engine.

Elasticsearch is an indexing and search technology, commonly used in companies when large volumes of data are processed. The CNIL has noted that servers using this technology are increasingly the target of attacks, and reminds best practices to reduce these risks (e.g., user authentication by password, firewall and connection filtering rules, encryption of communications, disabling or restricting scripts).

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

09/01/2020 – [French Supervisory Authority](#) | [Charter](#) | [Investigations](#)

The French Supervisory Authority (CNIL) has published a charter on its investigation procedures in order to ensure greater transparency and efficiency.

The 18-pages charter answers the following questions, among others: How does the CNIL decide to carry out an investigation?; What are the powers and obligations of CNIL agents?; Is it possible to refuse an investigation of the CNIL?; How does an investigation take place?; What can the organization do after the investigation?; What are the principles applicable to CNIL agents?; What behavior is expected from the persons solicited during the investigation?

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

Germany

10/01/2020 – [Hamburg Supervisory Authority | Sanction | Collection of sensitive data from employees](#)

The Hamburg Data Protection Commissioner (HmbBfDI) fined a retail company €35.3 million for collecting and storing sensitive personal data from employees such as information about illnesses, religious beliefs and family issues.

According to the investigation of the HmbBfDI, data about the personal life of the company's employees has been collected comprehensively and extensively by supervisors since at least 2014 and stored on the company's network drive. The information stored on the network drive was accessible to up to 50 managers of the company and was used, among other things, to create a profile of the individual employee in order to evaluate the work performance and to make employment decisions.

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

09/10/2020 – [German Data Protection Conference | Resolution | Use of thermal imaging cameras in the context of Covid-19](#)

The German Data Protection Conference (DSK) published a resolution concerning the use of thermal imaging cameras and electronic temperature recording to control access to airports, stores, public authorities and the workplace in the context of Covid-19.

In the DSK's opinion, the use of such technology is permissible under the GDPR in limited cases only. In particular, the DSK believes that temperature measurement does not provide significant benefits in the prevention and/or detection of Covid-19 infections and therefore in many cases lacks the effectiveness and necessity required under the principle of proportionality as set out by the GDPR.

For further information: [DSK Website](#)

09/07/2020 – [Baden-Württemberg Supervisory Authority | Recommendations | Schrems II](#)

The Baden-Württemberg Supervisory Authority (LfDI Baden-Württemberg) has updated its recommendations on international data transfers following the Schrems II ruling.

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

09/07/2020 – [Baden-Württemberg Supervisory Authority | Q&A | Controller-processor guidelines](#)

The Baden-Württemberg Supervisory Authority (LfDI Baden-Württemberg) published its frequently asked questions on the European Data Protection Board's new controller-processor guidelines, to help companies determine their role when processing personal data.

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

Greece

09/07/2020 – [Greek Supervisory Authority | Remote education](#)

The Greek Supervisory Authority (HDPa) has issued an opinion on remote education and compliance with the GDPR.

In particular, the HDPa stresses that data processing implemented in the context of remote education is lawful as long as personal data related to the use of video and sound are not recorded.

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

Ireland

09/05/2020 – [Irish Supervisory Authority | Recommendations](#)

The Irish Supervisory Authority (DPC) has published its recommendations regarding third parties which accidentally receive personal data relating to other individuals.

The DPC issued three separate guidances respectively for individuals or organisations which accidentally receive data, and conversely for data controllers who have lost control of data to a third party.

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

Italy

09/04/2020 – [Italian Supervisory Authority | Decision | Requirements for the accreditation of certification bodies](#)

The Italian Supervisory Authority (Garante) has published its requirements for the accreditation of certification bodies.

The Garante stressed that the requirements include, among other things, the absence of conflicts of interest and regular monitoring of certified products and services. As a reminder, certification is a procedure by which a certification body will provide written certification that a product or service is compliant with regulations.

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

Norway

09/09/2020 – [Norwegian Supervisory Authority | Sanction | Data Security](#)

The Norwegian Supervisory Authority fined the municipality of Bergen NOK 3 million (approx. €90,000) for failing to take adequate measures to ensure the protection of personal data.

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

Poland

09/08/2020 – [Polish Supervisory Authority | Sanction | Data Security](#)

The Polish Supervisory Authority fined the University of Warsaw PLN 50,000 (approx. €11,200) following a personal data breach which was notified in November 2019.

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

Romania

09/28/2020 – [Romanian Supervisory Authority | Annual Report](#)

The Romanian Supervisory Authority (ANSPDCP) has released its annual activity report for 2019.

In particular, the ANSPDCP noted that the efforts of public and private entities in 2019 focused on complying with data subjects' rights, as well as on ensuring data confidentiality and security.

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

Spain

09/17/2020 – [Spanish Law](#) | [Passenger names](#)

Spanish Law No. 1/2020 on the Use of Data from the Passenger Name Registry for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crimes was published in the Official Gazette.

The law notably aims to regulate the processing of data from the passenger name registry, including the transfer of data to competent authorities, EU Member States and third countries.

For further information: [Law No. 1/2020](#)

United Kingdom

09/24/2020 – [UK Supervisory Authority](#) | [Regulatory approach in response to the COVID-19 pandemic](#)

The British Supervisory Authority (ICO) published its updated regulatory approach in response to the COVID-19 pandemic, setting out how it will regulate in the coming months.

The ICO underlines that this update is another step towards returning to its approach before the COVID-19, but with the caveats and exceptions that reflect today's reality.

For further information: [UK Supervisory approach](#)

09/24/2020 – [UK Supervisory Authority](#) | [Sanction](#) | [Unsolicited marketing texts](#)

The British Supervisory Authority (ICO) fined a company £60,000 (approx. €66,000) for sending thousands of text messages advertising hydroalcoholic gel without consent at the height of COVID-19.

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

09/18/2020 – [UK Supervisory Authority](#) | [Guidance](#) | [Organisations mandated to collect customer information](#)

The UK Government has made it mandatory for all businesses in the hospitality sector, leisure and tourism sector and close contact businesses to collect customer information for the test and trace programme. In this context, the British Supervisory Authority (ICO) published guidance to collect such information.

GIBSON DUNN

The guidance notably advises organisations to collect only the specific information listed in the government's recommendation, not to re-use the data for other purposes, and to delete them after 21 days.

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

09/11/2020 – [UK Supervisory Authority | Framework | Accountability](#)

The British Supervisory Authority (ICO) published an accountability framework setting out its expectations of how organizations can demonstrate compliance with data protection regulations.

The framework sets out the ICO's key expectations and a non-exhaustive list of ways in which organisations can meet them. In addition, the framework includes a self-assessment function that allows organizations to evaluate the extent to which they are complying with the accountability principle.

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

09/10/2020 – [UK Supervisory Authority | Sanction | Direct marketing calls](#)

The British Supervisory Authority (ICO) fined a company £130,000 (approx. €140,700) for making more than 100,000 unauthorised pensions cold calls without the data subjects' consent between January 2019 and April 2019.

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

Others

08/21/2020 – [Irish Council for Civil Liberties | Complaint | New evidence](#)

The Irish Council for Civil Liberties (ICCL), an independent human rights campaigning organization, announced that it has submitted to the Irish Supervisory Authority (DPC) new evidences of a data breach occurring in the Google's Real Time Bidding system.

For further information: [ICCL Website](#)

09/03/2020 – Norwegian Parliament | Cyberattack

According to IAPP's website, hackers attacked the Norwegian Parliament's internal e-mail system, compromising the accounts of elected representatives and employees.

For further information: [IAPP 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*

***Penny Madden**, Partner, London - pmadden@gibsondunn.com*

***Michael Walther**, Partner, Munich - mwalther@gibsondunn.com*

***Kai Gesing**, Of counsel, Munich - kgesing@gibsondunn.com*

***Alejandro Guerrero**, Of counsel, Brussels - aguerrero@gibsondunn.com*

***Vera Lukic**, Of counsel, Paris - vlukic@gibsondunn.com*

***Sarah Wazen**, Of counsel, London - swazen@gibsondunn.com*

***Adélaïde Cassanet**, Associate, Paris - acassanet@gibsondunn.com*

***Franziska Gruber**, Associate, Munich - fgruber@gibsondunn.com*

***Selina Grün**, Associate, Munich - sgruen@gibsondunn.com*

***Clémence Pugnet**, Associate, Paris - 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.