

GIBSON DUNN PARIS | DATA PROTECTION – AUGUST 2020

To Our Clients and Friends:

Personal Data Watch

European Union

07/27/2020 – [EDPS | Opinion | Prevention of money laundering and terrorism financing](#)

The European Data Protection Supervisor (EDPS), Wojciech Wiewiórowski, reacted to the European Commission’s action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, released on May 7.

The EDPS believes that data protection requirements must go hand in hand with the prevention of money laundering and terrorism financing.

For further information: [EDPS Press Release](#)

07/23/2020 – [Court of Justice of the European Union | Ruling | Schrems II | Data transfers | Opinions of the authorities | EDPB FAQ](#)

On July 16, the Schrems II ruling issued by the Court of Justice of the European Union struck down as legally invalid the U.S.-EU Privacy Shield. The Court also ruled that the “data controller to data processor” Standard Contractual Clauses (SCCs) approved by the European Commission remain valid and may be used as an appropriate safeguard for data transfers to a third country, provided that a level of protection equivalent to that guaranteed within the EU may be ensured in the third country concerned.

Following this ruling, several supervisory authorities shared their opinions. Most of them, including the French Supervisory Authority (CNIL), the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), and the Luxembourg Supervisory Authority (CNPD), have indicated that they are currently carrying out a detailed analysis of the ruling, together with their European counterparts within the European Data Protection Board (EDPB), in order to assess its consequences for data transfers from the European Union to the United States.

The UK Supervisory Authority (ICO) invited companies currently using Privacy Shield to continue transferring data on this basis until new guidance becomes available, but updated its advice on July 27

to note that the the EDPB had issued Frequently Asked Questions on the invalidation of the Privacy Shield which still applied to UK controllers and processors, and the EDPB had recommended that a risk assessment must be undertaken as to whether SCCs provide enough protection within the local legal framework.

The BfDI, the German Data Protection Conference (DSK) and several other supervisory authorities in Germany have stated that companies can no longer transfer personal data on the basis of the Privacy Shield (and that data may need to be retransferred to the EU according to the Berlin data protection authority). In its initial reaction, the DSK has also specified that SCCs and BCRs require further evaluation and generally do not form a sufficient basis for data transfers to the United States without additional protective measures in place.

At the same time, the U.S. Department of Commerce stated that it will continue to administer the Privacy Shield program, including processing submissions for certification. In particular, on July 31, the International Trade Administration updated its Frequently Asked Questions in relation to the Privacy Shield, where it clarified that the Schrems II ruling does not relieve participants in the Privacy Shield of their obligations under the framework, and that the U.S. remains committed to working with the EU to ensure continuity in data flows and privacy protections.

On July 23, the EDPB issued Frequently Asked Questions stating in particular (i) that no "grace" period is granted for entities which rely on the Privacy Shield (another mechanism should therefore be put in place immediately); (ii) for SCCs and Binding Corporate Rules, the data controller should contact its processor to ensure the level of protection required by EU law is respected in the third country concerned (if not, the controller or the processor is responsible for determining what supplementary measures would ensure an equivalent level of protection, the EDPB adding that it will specify in further guidelines the supplementary measures that could be provided); and (iii) should the controller or processor determine that the data transferred are not afforded a level of protection essentially equivalent to that guaranteed within the EU, the transfer must be immediately suspended (if a company is willing to keep transferring data despite this conclusion, the competent supervisory authority must be notified).

For more information: [Press Release](#) | [Ruling](#) | [Gibson Dunn Website](#) | [EDPB FAQ](#)

07/30/2020 – [Council of the EU](#) | [Decision](#) | [Sanctions against cyber-attackers](#)

The Council of the EU imposed the first ever sanctions against cyber-attacks.

The Council has imposed restrictive measures against six individuals and three entities responsible for or involved in various cyber-attacks. These include the attempted cyber-attack against the OPCW (Organisation for the Prohibition of Chemical Weapons) and those publicly known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper'. The sanctions imposed include a travel ban and an asset freeze. In addition, EU individuals and entities are forbidden from making funds available to those listed.

For further information: [Council Statement](#) | [Decision](#)

07/23/2020 – [EDPB | Statement | Brexit](#)

The European Data Protection Board (EDPB) published an information note on Binding Corporate Rules approved by the UK Supervisory Authority (ICO).

The EDPB has outlined the actions that need to be taken to ensure that the Binding Corporate Rules approved by the ICO can still be used as a valid transfer tool, following the end of the transition period in relation to Brexit.

The statement however clarifies that this information note is without prejudice to the analysis currently undertaken by the EDPB on the consequences of the Schrems II ruling.

For further information: [EDPB Statement | Information Note](#)

07/20/2020 – [EDPB | Statement | PSD2](#)

The European Data Protection Board (EDPB) adopted guidelines on the interplay between the second Payment Services Directive (PSD2) and the GDPR, as well as a response letter to MEP Ľubomír Nicholsonová on contact tracing, interoperability of apps and data protection impact assessments.

For further information: [EDPB Website](#)

07/17/2020 – [High-Level Expert Group on Artificial Intelligence | Assessment List](#)

The High-Level Expert Group on Artificial Intelligence (AI HLEG) presented their final Assessment List for Trustworthy Artificial Intelligence.

The Group, set up by the European Commission, published its Assessment List designed to help businesses control the risks of the Artificial Intelligence systems they develop or acquire.

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

07/09/2020 – [European Commission | Communication | Brexit](#)

The European Commission published a communication on readiness at the end of the transition period between the EU and the UK, on December 31, 2020.

The Commission has advised companies to take the necessary steps to ensure the compliance of any personal data transfers to the UK with the GDPR, irrespective of the scenario whereby an EU adequacy decision will be taken with regard to the UK at the beginning of 2021.

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

07/09/2020 – [Court of Justice of the European Union | Ruling | GDPR Scope](#)

The Court of Justice of the European Union ruled that the Petitions Committee of the Parliament of a German Land is subject to the GDPR.

The ruling clarifies that no exception laid down by the GDPR applies to the Petitions Committee of the Parliament of a Federated State of a Member State, and that the Committee shall be considered as a controller. Citizens who have submitted a petition to that Committee therefore have, in principle, a right of access to their personal data.

For further information: [Press Release | Ruling](#)

07/07/2020 – [EDPB | Guidelines | Right to be Forgotten](#)

The European Data Protection Board (EDPB) adopted guidelines (05/2019) on the criteria of the right to be forgotten in the search engines cases under the GDPR.

These guidelines provide for the grounds a data subject may rely on for a delisting request sent to a search engine, as well as for the exceptions to the right to be forgotten.

For further information: [EDPB Guidelines 05/2019](#)

07/06/2020 – [EDPS | Report | Impact Assessments](#)

The European Data Protection Supervisor (EDPS), Wojciech Wiewiórowski, published a Report on how EU institutions carry out data protection impact assessments when processing information that presents a high risk to the rights and freedom of individuals.

For further information: [EDPS Press Release | EDPS Report](#)

07/06/2020 – [German Presidency of the Council of the European Union](#) | [Discussion Paper](#) | [ePrivacy Regulation](#)

The German Presidency of the Council of the European Union published a discussion paper regarding upcoming work on a potential ePrivacy Regulation.

Based on the latest proposal for an ePrivacy Regulation from March 6, 2020, the Presidency aims to reach a consensus among the EU Member States and/or a mandate to start negotiations on the proposed Regulation with the European Parliament. The Presidency has indicated that settling on core provisions of the ePrivacy proposal, particularly the rules on the processing of electronic communications data and the protection of end-users' terminal equipment information, is a key precondition to any agreement.

For further information: [Presidency Discussion Paper](#)

07/02/2020 – [EDPS](#) | [Public Paper](#) | [Microsoft](#)

The European Data Protection Supervisor (EDPS), Wojciech Wiewiórowski, published a Public Paper on the use of Microsoft products and services by EU institutions.

For further information: [EDPS Press Release](#) | [EDPS Public Paper](#)

Belgium

07/14/2020 – [Belgian Supervisory Authority](#) | [Sanction](#) | [Right to be Forgotten](#)

The Belgian Supervisory Authority imposed a fine of €600,000 on Google Belgium for violating the right to be forgotten and lack of transparency.

The authority sanctioned Google's refusal to delist links containing negative information about a Belgian citizen. The sanction also states that Google lacked transparency in its delisting form, as well as in its response to the data subject. This is the highest fine ever imposed by the Belgian authority.

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

Denmark

07/28/2020 – [Danish Supervisory Authority](#) | [Sanction](#) | [Data retention](#)

The Danish Supervisory Authority proposed to fine a hotel group DKK 1.1 million (around €147,500) for failing to delete approximately 500,000 customer profiles.

The Authority reported to the police that the customer profiles were kept in breach of the company's own deletion deadlines.

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

07/01/2020 – [Danish Supervisory Authority | Investigation | TikTok](#)

The Danish Supervisory Authority announced it is investigating TikTok.

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

France

07/28/2020 – [French Supervisory Authority | Standards and Guidance | Data processing and retention in the health sector](#)

The French Supervisory Authority (CNIL) adopted three standards for the health sector and published a guide on data retention.

The CNIL has adopted three standards for the health sector, which include a non-binding standard on the processing of personal data by medical and paramedical clinics, and two standards on data retention periods, applicable to processing activities in the health sector outside of the research domain and to processing activities for the purposes of research, study, and analysis in the health sector.

The CNIL has also published a practical guide on data retention periods in general, which covers topics such as the principle of data minimisation, the definition of retention periods, and retention period standards.

For further information: [CNIL Website | Guide](#)

07/24/2020 – [French Law | Marketing Calls](#)

The French law n° 2020-901 to regulate marketing calls and prevent fraudulent calls was officially enacted on July 24.

This law aims to strengthen the protection of consumers who may be victims of excessive marketing calls or fraudulent practices. A decree has yet to determine the days, times and frequency at which marketing calls will be allowed.

For further information: [Legifrance Website](#)

07/24/2020 – [French Supervisory Authority | Code of conduct | Accreditation requirements for monitoring bodies](#)

The French Supervisory Authority (CNIL) published its accreditation requirements for monitoring bodies, along with a Frequently Asked Questions.

Under article 41 of the GDPR, bodies which monitor compliance with a code of conduct must be accredited to this end by the competent supervisory authority. In this context, the CNIL has adopted its accreditation requirements, which relate in particular to the independence of the monitoring body, the appropriate level of expertise of the auditors, specific security measures, transparent handling of complaints, regular monitoring procedures as well as procedures for the adoption of sanctions.

For further information: [CNIL Website](#)

07/20/2020 – [French Supervisory Authority | « StopCovid » App | Notice](#)

Following its investigations into the "StopCovid" app, the French Supervisory Authority (CNIL) has found that the new version of the app is mainly compliant with the GDPR and the French Data Protection Act.

However, the CNIL has identified certain breaches and has given the Ministry of Solidarity and Health formal notice to remedy them. In particular, the CNIL noted certain specific breaches related to data protection impact assessment, the information provided to users and data processing agreements.

For further information: [CNIL Website](#)

07/10/2020 – [French Supervisory Authority | Guidance | Authorized Third Parties](#)

Certain authorities known as "authorized third parties" have the power to require entities to provide documents or information that may include personal data. The French Supervisory Authority (CNIL) published guidance on handling data transfer requests from authorized third parties.

Before responding to an authorized third party, the CNIL has advised organizations to obtain a written communication detailing the legal basis as well as the control, confidentiality and traceability measures implemented for the procedure. The CNIL has also published a table of the main procedures that may be implemented by authorized third parties.

For further information: [CNIL Website](#)

07/09/2020 – [French Supervisory Authority | Best Practices](#)

The French Supervisory Authority (CNIL) published six best practices for data controllers and processors handling personal data.

These best practices relate in particular to the determination of the status of the actors involved in the data processing and the conclusion of a transparent agreement.

For further information: [CNIL Website](#)

Germany

07/27/2020 – [German Federal Court of Justice | Ruling | Right to be Forgotten](#)

The German Federal Court of Justice denied the plaintiff a “Right-to-be-forgotten” arguing that his fundamental rights do not outweigh the interests of the defendant and the public.

In this case, the plaintiff requested that the defendant, a search engine, delist certain press articles about the defendant in the search results list. The Court stated that the “Right-to-be-forgotten”, codified within Art. 17 GDPR, requires a comprehensive balancing of fundamental rights of both the plaintiff and the defendant. As a result, the Court denied the plaintiff’s claim since the interests of the defendant and the public outweighed the plaintiff’s right to privacy and right to protection of his personal data. In a related case, the Court referred two questions on the interpretation of article 17 of the GDPR to the Court of Justice of the European Union.

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

07/17/2020 – [Federal Constitutional Court | Ruling | Telecommunications Act](#)

In an order published on July 17, the Federal Constitutional Court in Karlsruhe declared unconstitutional a provision of the Telecommunications Act on the grounds that it violates citizens' rights to informational self-determination and the privacy of telecommunications.

The order concerned the current provision, under which security authorities could obtain data from telecommunications providers for various non-specific purposes without the approval of a judge. The unconstitutional provision is still in force, however the government must amend the act by the end of 2021.

For further information: [German Federal Constitutional Court Website](#)

07/03/2020 – [Berlin Commissioner for Data Protection and Freedom of Information \(BlnBDI\) | Guidance | Assessment of Video Conferencing Services with regard to Data Processing Agreements](#)

The Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI) published an assessment of various video conferencing services focusing on the conformity of the data processing agreements with the GDPR.

The document published by the BlnBDI provides an overview of various video conferencing services and the respective underlying data processing agreements. According to the BlnBDI, many of the data processing agreements contain deficiencies that would preclude the use of the respective service in compliance with GDPR principles.

For further information: [BlnBDI Website](#)

Italy

07/09/2020 – [Italian Supervisory Authority | Sanction | Direct Marketing](#)

The Italian Supervisory Authority fined a telecommunication operator and one of its business partners €16,700,000 and €200,000 respectively.

After an investigation, the Italian Supervisory Authority found that hundreds of data subjects received unsolicited communications, sent without their prior consent and without being able to exercise their right to object to the processing. In other cases, the data collected were published on public telephone lists despite the objection of the data subjects. The investigation also showed that several apps distributed by the company were set up in such a way that the user was forced to consent to various processing activities each time he/she accessed the apps, with the possibility of withdrawing consent only after 24 hours.

One of the operator's business partners was also sanctioned for unlawful subcontracting of processing activities to third party call centers.

It is worth noting that, on the same day, the Italian Supervisory Authority fined another telecom operator €800,00.

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

Norway

07/02/2020 – [Norwegian Supervisory Authority](#) | [Sanction](#) | [Impact Assessment](#)

The Norwegian Supervisory Authority fined Rælingen municipality NOK 500,000 (around €46,500) for the processing of health data relating to children's disability without carrying out a data protection impact assessment prior to the processing, and without implementing adequate technical and organisational measures.

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

Romania

07/09/2020 – [Romanian Supervisory Authority](#) | [Sanction](#) | [Security Measures](#)

The Romanian Supervisory Authority fined a company €15,000 for failing to implement appropriate security measures.

The authority states that the investigation follows the notification of a data breach affecting 436 data subjects, the company having published on Facebook the password allowing access to the forms filled in by participants in a contest.

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

Spain

07/28/2020 – [Spanish Supervisory Authority](#) | [Guidance](#) | [Cookies](#)

The Spanish Supervisory Authority (AEPD) updated its guidance on the use of cookies.

The AEPD announced the publication of an updated version of its guide on the use of cookies in order to adapt it to the EDPB's Guidelines 05/2020 on Consent under the GDPR. In particular, the AEPD incorporates to the guide that cookie walls cannot be used, since they do not offer a valid alternative to consent, and that continued browsing cannot constitute a valid way to obtain consent.

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

07/08/2020 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Right of Access](#)

The Spanish Supervisory Authority (AEPD) fined a company €40,000 for failing to give a data subject access to his telephone records, despite the authority’s notice.

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

United Kingdom

07/30/2020 – [UK Supervisory Authority](#) | [Guidance](#) | [AI and Data Protection](#)

The UK Supervisory Authority (ICO) announced the release of Guidance on AI and data protection as part of wider AI framework.

The blog post announced the issuance of guidance on AI and data protection as part of its wider efforts on an AI framework, which aims at offering a methodology for auditing AI to ensure personal data is fairly processed. The guidance covers the accountability and governance implications of AI; requirements for ensuring lawfulness, fairness, and transparency in AI systems; assessments for security and data minimisation in AI; and methods for ensuring individual rights are respected within AI systems. The guidance is aimed at professionals with a focus on compliance (e.g., DPO) and technology specialists.

For further information: [ICO Website](#)

07/20/2020 – [UK Supervisory Authority](#) | [Annual Report](#)

The UK Supervisory Authority (ICO) released its 2019-2020 annual report.

The report looks back at the various actions taken by the ICO for the 2019-2020 period, which Information Commissioner Elizabeth Denham has called a “transformative period” for privacy and data protection and broader information rights, but she added: “The law has not changed, and the ICO continues to be a proportionate and practical regulator.”

For further information: [ICO Website](#)

07/09/2020 – [UK Supervisory Authority](#) | [Investigation](#) | [Clearview AI Inc.](#)

The Australian Supervisory Authority (OAIC) and the UK Supervisory Authority (ICO) opened a joint investigation into Clearview AI Inc.

In its statement, the ICO has indicated that the investigation will focus on Clearview's data-scraping practices and its use of biometric information.

For further information: [OAIC Website](#)

Others

07/31/2020 – [Facebook](#) | [Complaint](#) | [European Commission](#)

According to IAPP's website, Facebook has filed lawsuits against EU antitrust regulators, for allegedly requesting information in breach of its employees' privacy, in the context of their investigations into the company's practices.

For further information: [IAPP Website](#)

07/02/2020 – [CNIL](#) | [Complaint](#) | [Doctissimo](#)

The NGO Privacy International has reportedly filed a complaint with the French Supervisory Authority (CNIL) against Doctissimo for various breaches of data protection regulation.

For further information: [Privacy International 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

GIBSON DUNN

© 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.