

January 13, 2022

GIBSON DUNN | EUROPE | DATA PROTECTION – DECEMBER 2021 (PART 2)

To Our Clients and Friends:

Personal Data Watch

Europe

12/17/2021 – [European Commission | Adequacy Decision | Data Transfers to South Korea](#)

The European Commission adopted the South Korean adequacy decision, making it possible for personal data to travel from the European Union to the Republic of Korea without any need for additional tools or authorizations.

By this decision, the Commission attests that the South Korean legislation on data protection (the Personal Information Protection Act) combined with the additional safeguards implemented, guarantees a comparable level of protection of personal data to that in the European Union.

For further information: [Commission Website](#)

12/16/2021 – [European Data Protection Board | Statement | Elaboration of Guidelines](#)

The European Data Protection Board adopted a statement regarding the cooperation on the elaboration of guidelines.

The Board highlights that, although not binding in themselves, its guidelines and recommendations reflect the common position which the authorities agree to apply in a consistent way.

For further information: [EDPB Website](#)

12/14/2021 – [European Data Protection Board | Guidelines | Data Breach Notification](#)

The European Data Protection Board adopted the final version of its Guidelines 01/2021 on Examples regarding Personal Data Breach Notification after public consultation.

The Guidelines aim to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment. Though the cases presented in the Guidelines are fictitious, they are based on typical cases from the supervisory authorities' collective experience with data breach notifications.

For further information: [EDPB Website](#)

12/14/2021 – [European Data Protection Board | Contribution | Data Protection Law Enforcement Directive](#)

The European Data Protection Board issued a contribution to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 of the GDPR.

As a reminder, the LED aims to provide a harmonized level of data protection for individuals in the area of law enforcement across the EU. In its contribution, the EDPB strongly urges Member States to ensure that their transposition is fully compliant with the LED without any further delays, and that supervisory authorities are provided with enough resources to ensure the effective implementation of the LED.

For further information: [EDPB Website](#)

12/14/2021 – [European Data Protection Board | Letter | Pegasus Spyware](#)

The European Data Protection Board issued a letter regarding the hacking spyware Pegasus.

The Board highlights that it pays particular attention to the current developments related to the interferences with the fundamental rights to privacy and data protection through surveillance measures. The Board adds that the Hungarian Supervisory Authority has competency to carry out the investigation procedure regarding the alleged use of spyware by Hungarian authorities, but that it remains ready to provide support in such matters.

For further information: [EDPB Website](#)

Czech Republic

12/22/2021 – [Czech Supervisory Authority | FAQs | Cookies](#)

The Czech Supervisory Authority published FAQs on obtaining consent for the use of cookies through cookie banners.

For further information: [UOOU Website](#)

France

12/28/2021 – [French Supervisory Authority | Fine | Data Subjects' Rights](#)

The French Supervisory Authority imposed a €300,000 fine to a French telecom operator for failure to comply with data subjects' rights and data security requirements.

According to the decision, the company failed to comply with data subjects' right of access and to object to processing for direct marketing purposes. The company would have also breach the principles of privacy by design and data security, insofar as unencrypted passwords were transmitted by email.

For further information: [CNIL Decision](#)

12/30/2021 – [French Supervisory Authority | Fine | Data Breach](#)

The French Supervisory Authority imposed a €180,000 fine to a fintech startup for failure to ensure the security of personal data and to inform data subjects of a data breach.

The Authority explains that personal data used for one of the company's internal research project remained stored on an online server with unrestricted access from 2016 to 2020. The data breach affected 12 million individuals located in several European countries. Following the investigation, the Authority also found other breaches, including a failure to comply with the requirements regarding data processing agreements.

For further information: [CNIL Website](#)

12/16/2021 – [French Supervisory Authority | Formal Notice | Biometric Data](#)

The French Supervisory Authority issued a formal notice against an American AI company specialized in facial recognition to stop further processing and delete personal data of French individuals.

As a reminder, the company uses data scraped from the internet for facial recognition and has already been subject to enforcement actions, including in Australia, the UK and Canada.

The Authority considers that the company has processed biometric data without a legal basis and has failed to facilitate the exercise of data subject rights. It also considers that each supervisory authority is competent to act on its own territory due to the lack of establishment of the company in Europe.

For further information: [CNIL Website](#)

12/14/2021 – [French Supervisory Authority](#) | [Statement](#) | [Cookies](#)

The French Supervisory Authority issued a statement on its past and future enforcement actions to ensure compliance with the rules on cookies.

As a reminder, since May 2021, the Authority has regularly issued formal notices to companies that do not allow to refuse cookies as easily as to accept them. The Authority's statement outlines that formal notices have been issued to ninety companies so far, and that the Authority will continue its controls and pronounce the necessary corrective measures.

For further information: [CNIL Website](#)

12/13/2021 – [French Supervisory Authority](#) | [Guidance](#) | [Developers](#)

The French Supervisory Authority updated its guidance dedicated to developers.

The Authority highlights that this major revision includes new content as regards cookies and security measures, including snippets of code illustrating GDPR requirements.

For further information: [CNIL Website](#)

12/01/2021 – [French Supervisory Authority](#) | [Guidance](#) | [Multi-Factor Authentication](#)

The French Supervisory Authority published guidance on the use of multi-factor authentication for online accounts.

The Authority notably recommends activating multi-factor authentication each time a service offers it, although it acknowledges that this mechanism remains vulnerable to certain sophisticated attacks such as real-time phishing.

For further information: [CNIL Website](#)

Germany

12/20/2021 – [German Data Protection Conference](#) | [Guidance](#) | [Telecommunications](#)

The German Data Protection Conference (DSK) published guidance on the new German Data Protection and Privacy in Telecommunications and Telemedia Act (TTDSG).

As a reminder, the TTDSG entered into force on 1 December 2021. The guidance notably clarifies the interplay between the TTDSG and the GDPR, and provides assistance to operators of websites, apps, and smart home applications in the implementation of the new provisions of the TTDSG. The DSK consists of the 16 data protection supervisory authorities in Germany.

For further information: [DSK Guidance](#)

12/15/2021 – [Bavarian Supervisory Authority](#) | [Handout](#) | [Log4Shell Vulnerabilities](#)

The Bavarian Supervisory Authority published a handout describing required remedial measures and providing information for an initial assessment for controllers being affected by the critical IT-security vulnerability “Log4Shell”.

The authority also announces that it may conduct and intensify data security audits.

For further information see: [BayLDA Handout](#)

12/01/2021 – [Administrative Court of Wiesbaden](#) | [Decision](#) | [Data Transfers](#)

The Administrative Court of Wiesbaden issued a preliminary injunction which prohibits a university from using a cookie consent management tool which transferred personal data to the U.S. without appropriate safeguards.

The decision highlights that the provider of the cookie banner relied on U.S. processors, and thus transferred individuals’ complete IP addresses to the U.S. without a transfer mechanism in place.

For further information: [Court Website](#)

Iceland

12/15/2021 – [Icelandic Supervisory Authority | 2020 Annual Report](#)

The Icelandic Supervisory Authority issued its 2020 Annual Report.

For further information: [Persónuvernd Website](#)

Ireland

12/22/2021 – [Irish Supervisory Authority | Report | Regulatory Strategy](#)

The Irish Supervisory Authority published its Regulatory Strategy for 2022-2027.

The main objectives of the Authority for the next years are to (i) regulate consistently and effectively, (ii) safeguard individuals and promote data protection awareness, (iii) prioritize the protection of children and other vulnerable groups, (iv) bring clarity to stakeholders, and (v) support organizations and drive compliance.

For further information: [DPC Website](#)

12/20/2021 – [Irish Supervisory Authority | Report | Audit](#)

The Irish Supervisory Authority published a report on data protection audit of political parties in Ireland.

The report highlights the main findings of the audits conducted this year in 26 registered political parties given the public interest in this matter, and outlines the key recommendations made by the Authority to the political parties concerned.

For further information: [DPC Website](#)

12/17/2021 – [Irish Supervisory Authority | Guidance | Children Data](#)

The Irish Protection Authority published the final version of its guidance on children data processing.

The guidance introduces child-specific principles and recommended measures to address the data processing risks posed by children's access to services in both an online and offline world. In this respect, the Authority identifies 14 so-called Fundamentals that organizations should follow, including child-

oriented transparency or the fact that theoretical user age thresholds do not displace organizations' obligations.

For further information: [DPC Website](#)

Italy

12/03/2021 – [Italian Supervisory Authority](#) | [Sanction](#) | [Employee Monitoring](#)

The Italian Supervisory Authority published a decision issued on 28 October 2021, imposing a €30,000 fine to a public transportation company for unlawful monitoring of its call center employees.

The Authority highlights that the company parametered its call management system to allow the monitoring of employees' work, including the recording and unlimited storage of calls, in breach of the principles of minimization and limitation of the data retention period.

For further information: [Garante Website](#)

12/03/2021 – [Italian Supervisory Authority](#) | [Sanction](#) | [Right of Access](#)

The Italian Supervisory Authority published a decision issued on 11 November, imposing a €150,000 fine to an Italian telecom company for violating the right of access of an individual.

For further information: [Garante Decision](#)

Netherlands

12/21/2021 – [Dutch National Ombudsman](#) | [Report](#) | [Authority's Handling of Privacy Complaints](#)

The Dutch National Ombudsman published a report criticizing the Dutch Supervisory Authority handling of citizens' privacy complaints.

The report highlights the Authority's lack of practical approach and makes several recommendations, including providing citizens with more clarity about the status of a decision and how to challenge it, as well as using more clear and understandable language.

For further information: [Ombudsman Website](#)

12/08/2021 – [Dutch Supervisory Authority](#) | [Sanction](#) | [Unlawful Processing by Tax Administration](#)

The Dutch Supervisory Authority imposed a €2.75 million fine on the Dutch Tax Administration for processing data on the dual nationality of childcare benefit applicants in an unlawful and discriminatory manner.

For further information: [DPA Website](#)

Norway

12/21/2021 – [Norwegian Supervisory Authority](#) | [Sanction](#) | [Data Sharing](#) | [Behavioral Advertisement](#)

The Norwegian Supervisory Authority fined the provider of a dating application NOK 65 million (approx. €6.5 million) for not complying with the GDPR rules on consent.

The decision considers that the company has disclosed user data to third parties for behavioral advertisement without a legal basis, since the company did not collect a specific consent for that purpose and the related information was not properly communicated to users.

For further information: [Datatilsynet Website](#)

Spain

12/21/2021 – [Spanish Supervisory Authority](#) | [Sanction](#) | [Legal Basis](#)

The Spanish Supervisory Authority fined a bank €100,000 for processing personal data without a valid legal basis.

For further information: [AEPD Website](#)

United Kingdom

12/21/2021 – [UK Supervisory Authority](#) | [Nomination](#) | [Commissioner](#)

John Edwards, the former New-Zealand Privacy Commissioner, was confirmed as the new UK Information Commissioner as of 3 January 2022.

For further information: [ICO Website](#)

GIBSON DUNN

12/17/2021 – [UK Supervisory Authority](#) | [Sanction](#) | [Direct Marketing Calls](#)

The UK Supervisory Authority fined a gas company £75,000 (approx. €90,000) for making direct marketing calls to subscribers on do-not-call lists and who had not provided valid consent.

For further information: [ICO Website](#)

12/08/2021 – [UK Supervisory Authority](#) | [Sanction](#) | [Consent](#)

The UK Supervisory Authority fined a telecommunication company £50,000 (approx. €60,000) for sending around 450,000 direct marketing messages to individuals who had previously opted out of marketing communications.

For further information: [ICO Website](#)

12/02/2021 – [UK Supervisory Authority](#) | [Sanction](#) | [Data Breach](#)

The UK Supervisory Authority fined the Cabinet Office £500,000 (approx. €600,000) for disclosing online the postal addresses of the 2020 New Year Honors recipients.

For further information: [ICO Website](#)

12/01/2021 – [UK Supervisory Authority](#) | [Sanction](#) | [Marketing Calls](#)

The UK Supervisory Authority fined a financial company £140,000 (approx. €160,000) for instigating around 100,000 cold calls to people about pensions without valid consent.

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, PCDA 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)

Vera Lukic – Partner, Paris (vlukic@gibsondunn.com)

Penny Madden – Partner, London (pmadden@gibsondunn.com)

GIBSON DUNN

Michael Walther – Partner, Munich (mwalther@gibsondunn.com)
Alejandro Guerrero – Of counsel, Brussels (aguerrero@gibsondunn.com)
Sarah Wazen – Of counsel, London (swazen@gibsondunn.com)
Clémence Pugnet – Associate, Paris (cpugnet@gibsondunn.com)
Léna Bionducci – Associate, Paris (lbionducci@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.