GIBSON DUNN

December 22, 2021

GIBSON DUNN | EUROPE | DATA PROTECTION – DECEMBER 2021

To Our Clients and Friends:

Personal Data Watch

Europe

11/18/2021 – European Data Protection Board | Letter | Dialogue with the United Nations on Data Protection

The European Data Protection Board published a letter regarding the ongoing dialogue between the European Data Protection Board and the United Nations on data protection, in particular on international data transfers.

As a reminder, the European Data Protection Supervisor established a Task Force to informally address various issues relating to transfers to international organisations, with the participation of the United Nations. In this letter, the Board's Chair notably indicates that he will consider the United Nations' suggestion to address the situation in a specific set of guidelines.

For further information: EDPB Website

11/18/2021 – European Data Protection Board | Guidelines | International Data Transfers

The European Data Protection Board issued its new Guidelines 05/2021 on the interplay between the territorial scope of the GDPR and the provisions on international transfers, and opened a public consultation on the same.

The Guidelines aim to assist controllers and processors in identifying whether a processing constitutes a transfer to a third country and, as a result, whether they have to comply with the international data transfer provisions of the GDPR.

The Board elaborates on the three cumulative criteria to qualify a processing as an international transfer of personal data, namely: (i) a controller or a processor is subject to the GDPR for the given processing; (ii) this controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"); and (iii) the importer is in a third country or is an international organisation, irrespective of whether or not

this importer is subject to the GDPR in respect of the given processing. The Guidelines notably clarify that the second criterion cannot be considered as fulfilled where the data is disclosed directly and on his/her own initiative by the data subject to the recipient.

For further information: EDPB Website

11/18/2021 – European Data Protection Board | Statement | Digital Services Package and Data Strategy

The European Data Protection Board issued a statement on the Digital Services Package and Data Strategy proposed by the European Commission, which draws attention to a number of overarching concerns and urges the co-legislature to take decisive action.

As a reminder, since November 2020, the European Commission has presented several legislative proposals as part of its digital and data strategies. With this statement, the Board draws attention to three categories of concerns, namely: (i) the lack of protection of individuals' fundamental rights and freedoms; (ii) the fragmented supervision; and (iii) the risks of inconsistencies. The Board also urges the co-legislature to take decisive action insofar as it considers that, without further amendments, the proposals will negatively impact the fundamental rights and freedoms of individuals and lead to significant legal uncertainty.

For further information: EDPB Website

11/18/2021 – European Data Protection Board | Letter | Cybersecurity Certification for Cloud Services

The European Data Protection Board published a letter addressed to the European Union Agency for Cybersecurity (ENISA) regarding the European Cybersecurity Certification Scheme for Cloud Services.

In this letter, the Board requests the ENISA to take into account the Schrems II ruling for the final certification Scheme.

For further information: EDPB Website

Belgium

11/25/2021 – Belgian Supervisory Authority | Draft decision | Advertising

The Belgian Supervisory Authority announced that it has finalised its draft decision in the case against IAB Europe about the conformity of the so-called Transparency & Consent Framework (TCF) with the GDPR.

As a reminder, the TCF aims to contribute to the GDPR compliance of the OpenRTB protocol, which is one of the most widely used Real-Time Bidding protocols.

Given the cross-border nature of the TCF, the Belgian Authority is acting as the lead authority in this case. Accordingly, it has notified its draft decision to the 27 other concerned European supervisory authorities, who now have 4 weeks to provide feedback.

For further information: DPA Website

Denmark

11/05/2021 – Danish Business Authority | Statement | Electronic Communication

The Danish Business Authority stated that it will increase its supervision of messaging apps, dating sites, and other online services that allow their users to communicate with each other.

For further information: DBA Website

France

11/18/2021 – French Supervisory Authority | Recommendation | Logs

The French Supervisory Authority published the final version of its recommendation on logs following public consultation.

The Authority highlights that logging systems are essential tools for the security of personal data and can be used to detect incidents or unauthorised access.

The recommendation aims to guide data controllers in the implementation of these tools, in particular by clarifying the appropriate retention periods for logs.

For further information: CNIL Website

11/16/2021 – French Supervisory Authority | Guidance | Data Protection Officers

The French Supervisory Authority published a practical guide on data protection officers, compiling useful knowledge and good practices on the topic.

The guide contains principles, examples and practical resources on data protection officers' role, their appointment, their missions, and the tools that the CNIL makes available to them.

For further information: CNIL Website

11/10/2021 – French Supervisory Authority | Guidance | Associations

The French Supervisory Authority published a high-level guide for associations, which provides an overview of the main concepts and requirements of the GDPR.

For further information: CNIL Website

11/04/2021 – French Supervisory Authority | Sanction | Data Minimisation

The French Supervisory Authority published a decision issued on October 29, 2021, fining a public transport company €400,000 for breaches relating to employee evaluation files.

The Authority outlines that the evaluation files included the number of days employees had been on strike, in breach of the principles of data minimisation, limited data retention and data security.

For further information: CNIL Website

Germany

11/24/2021 – German Data Protection Conference | Decision | Security

The German Data Protection Conference published a decision, holding that it is neither possible for the controller to refrain from applying technical and organisational measures required by Article 32 of the GDPR at the express request of the data subject nor on the basis of its consent.

Having said that, the Authority specifies that it may be possible for the controller not to apply certain technical and organizational measures to a reasonable extent in individual and documented cases, subject to an explicit and informed request of the data subject concerned.

For further information: DSK Decision

11/24/2021 – New German Government | Coalition Agreement | Data Privacy Policy

The parties forming the new German Government published their coalition agreement, which contains the new Government's agenda regarding data privacy.

Among other initiatives, the new Government aims to strengthen European cooperation, to further institutionalize the German Data Protection Conference in the Federal Data Protection Act and to enable the German Data Protection Conference to enact binding decisions.

For further information: Coalition Agreement

11/16/2021 – Munich Regional Court | Decision | Right of access

The Munich Regional Court published a decision dated September 2, 2021, holding that a company duly fulfilled its obligation to answer data subjects' access requests by providing permanently available URL links directing individuals to their data.

For further information: Munich Regional Court Decision

11/01/2021 – Essen Regional Court | Decision | Assignment of damage claims

The Essen Regional Court published a decision dated September 23, 2021, in which it stated that claims for non-material damages under Article 82 of the GDPR may be assigned to third parties.

This statement holds particular relevance since it may facilitate the commercial bundling and enforceability in mass consumer litigation. Further, the Court held that even a formal violation of the GDPR, e.g. in this case a failure to notify a data breach to a competent data protection authority, may be sufficient to establish a claim for non-material damages.

For further information: Essen Regional Court Decision

Iceland

11/02/2021 – Icelandic Supervisory Authority | Decision | Domestic CCTV

The Icelandic Supervisory Authority published a decision dated October 27, 2021 finding that the installation of CCTV at a multi-family house breached the GDPR insofar as it was not necessary to monitor all covered areas.

For further information: Persónuvernd Website

Ireland

11/26/2021 – Irish Supervisory Authority | Statement | Data Protection Officer Enforcement Programme

The Irish Supervisory Authority issued a statement indicating that it has completed the most recent stage in its Data Protection Officer enforcement programme, which has brought more than 170 organizations into compliance with requirements on the topic.

With respect to private organisations, the Authority has focused its compliance checks on Private Hospitals & Out-of-Hours GP Services, Banking Entities, and Credit Unions. The Authority indicates that, in cases where it identifies persistent non-compliance, further enforcement measures will be taken and it will consider whether further guidance is necessary to address any issues of concern before extending compliance checks to other sectors.

For further information: DPC Website

11/22/2021 – Irish Supervisory Authority | Guidance | Domestic CCTV

The Irish Supervisory Authority published guidance on the use of domestic CCTV.

In this document, the Authority reminds the scope of the household exemption and sets out its general approach to the frequent complaints from individuals relating to the operation of domestic CCTV.

For further information: DPC Website

11/19/2021 – Irish Supervisory Authority | Public Consultation | Child-Oriented Approach to Data Processing

The Irish Supervisory Authority published a report compiling the results of its public consultation on the draft guidance entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing".

The Authority aims to provide an overview of the headline trends and themes emerging from stakeholders' submissions, as well as the Authority's responses to this feedback.

For further information: DPC Website

11/05/2021 – Irish Supervisory Authority | Form | New Breach Notification Form

The Irish Supervisory Authority (DPC) published a summary of changes to the breach notification form, which is now live on the DPC's website.

In particular, the new webform requires users to confirm whether the breach reaches the risk threshold for notification and whether the DPC is their lead supervisory authority and, if so, the basis for this assessment. Additionnally, it is now possible to upload any further information or supporting documentation.

For further information: DPC Website

11/02/2021 – Irish Supervisory Authority | Guidance | Vaccine Certificate Check

The Irish Supervisory Authority published guidance on vaccine certificate check.

The guidance clarifies when owners/operators of premises can check the Covid certificates of its customers or visitors, from the point of view of both the owners/operators of premises and of data subjects.

For further information: DPC Website

Italy

11/26/2021 – Italian Supervisory Authority | Sanction | Unlawful processing

The Italian Supervisory Authority published a decision, dated September 16, 2021, to fine a company €75,000 for carrying out unlawful processing of its employees' data through the use of video surveillance system.

The Company has notably failed to follow the adequate local procedure for the installation of the video surveillance equipment.

For further information: Garante Website

11/24/2021 – Italian Supervisory Authority | Sanction | Unlawful Processing

The Italian Supervisory Authority published a decision, dated September 29, 2021, to fine a media company €30.000 for publishing an article containing excessive personal data of an individual who was severely injured.

The article notably included identification and health data of the individual, as well as details on the trial and on the compensation paid to him by the insurance.

For further information: Garante Decision

Luxembourg

11/02/2021 – Luxembourg Supervisory Authority | Sanction | Data Protection Officer

The Luxembourg Supervisory Authority published a sanction decision dated October 13, 2021, which found that a company breached its obligations (i) to communicate the contact details of the data protection officer to the Authority, and (ii) to ensure that the other tasks the data protection officer fulfils do not result in a conflict of interests with its role.

For further information: CNPD Decision

Netherlands

11/12/2021 – Dutch Supervisory Authority | Sanction | Security of Processing

The Dutch Supervisory Authority published a decision issued on September 23, 2021 to fine an airline company €400,000 for insufficient personal data security.

The Authority outlines that a hacker was able to break into the company's systems in which he could access to the data of 25 million passengers, mainly due to three security flaws: (i) the password was easy to guess; (ii) there was no multi-factor authentication; and (iii) access rights were not restricted to necessary systems.

For further information: AP Website

Poland

11/08/2021 – Polish Supervisory Authority | Sanction | Personal Data Breach

The Polish Supervisory Authority published a decision issued on October 14, 2021 to fine a bank €80,000 for failure to notify a data breach to the competent supervisory authority and failure to fully comply with the obligation to communicate the data breach to data subjects.

The Authority outlines that if the controller had notified the supervisory authority in this case, it would have been informed that the breach should also be communicated to individuals. The decision also orders the communication of the breach to the data subjects affected.

For further information: UODO Website

Spain

11/16/2021 – Spanish Supervisory Authority | Sanction | Right to object

The Spanish Supervisory Authority published a decision, issued on October 6, 2021, to fine a telecommunications operator €15,000 for sending direct marketing communications to an individual after he exercised his right to object.

For further information: AEPD Website

United Kingdom

11/29/2021 – UK Supervisory Authority | Intent to Fine | Unlawful Processing of Biometric Data

The UK Supervisory Authority (ICO) announced its provisional intent to fine a company specialized in facial recognition £17 million, and issued a provisional notice to stop further processing and delete the personal data of people in the UK.

As a reminder, the ICO and the Office of the Australian Information Commissioner opened a joint investigation in July 2020 on the company's use of data scraped from the internet and the use of biometrics for facial recognition.
The ICO's preliminary view is that the company appears to have failed to comply with UK data protection laws in several ways including with regard to the principles of fairness, limited data retention, lawfulness and information.

For further information: ICO Website

11/25/2021 – UK Supervisory Authority | Opinion | Online advertising

The UK Supervisory Authority issued an opinion entitled "*Data protection and privacy expectations for online advertising proposals*", in collaboration with the UK Competition and Markets Authority.

The opinion aims to assess the industry's initiatives to shift towards less intrusive tracking and profiling practices. In particular, the Authority indicates that initiatives must address the risks that adtech poses and take account of data protection requirements from the outset. Any proposal that has the effect of maintaining or replicating existing tracking practices is not an acceptable response to the significant data protection risks that the Authority has already described.

For further information: ICO Website

11/10/2021 – UK Supreme Court | Judgment | Class Action

The UK Supreme Court issued a unanimous judgment in the *Lloyd v Google LLC* case, overturning a ruling of the Court of Appeal and disallowing a data privacy class action.

The Judgment denies Mr. Lloyd the ability to pursue a collective claim for compensation on behalf of around four million iPhone users in England and Wales whose internet activity data were allegedly collected by Google in late 2011 and early 2012 for commercial purposes without the users' knowledge or consent, and in alleged breach of the Data Protection Act 1998.

The Supreme Court's Judgment provides, in brief, that the procedural mechanism used to bring the claims on a collective basis (known as a "representative action") can be used for claims of this kind, but only for the purposes of establishing liability for a breach of relevant data protection laws. The question of damages cannot be addressed through a representative action, and would have to be dealt with through individual claims, which could be managed together through group litigation case management devices.

The Court held that a representative action is unsuitable for damages assessment in a case of this kind because (i) damages for mere loss of control of data (as distinct from damages for actual loss or distress caused by the data breach) are not available for breaches of the 1998 Act (although the Supreme Court intimated that they may have been for another tort, misuse of private information); and (ii) even if such damages had been available, assessment of loss can only be determined on the basis of an individualised assessment of the alleged misuse of each individual's data.

For further information: Supreme Court Website | Gibson Dunn Alert

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

Michael Walther *– Partner, Munich (mwalther@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)*
Clémence Pugnet *– Associate, Paris (cpugnet@gibsondunn.com)*
Selina Grün *– Associate, Munich (sgruen@gibsondunn.com)*
Léna Bionducci *– Associate, Paris (lbionducci@gibsondunn.com)*