GIBSON DUNN

April 9, 2020

GIBSON DUNN PARIS | DATA PROTECTION – APRIL 2020

To Our Clients and Friends:

Personal Data Watch

European Institutions

03/19/2020 – EDPB | Statement | COVID-19

The European Data Protection Board (EDPB) issued a statement on the processing of personal data in the context of the COVID-19 outbreak.

In its publication, the EDPB refers to the criteria for the lawfulness of the processing, outlines the main data protection principles and answers some questions relating to the processing of location data.

With respect to the lawfulness of the processing, the EDPB specifies the different legal basis that may apply in the context of an epidemic to allow employers and public health authorities to process personal data without the consent of individuals (i.e., processing in the public interest, processing to protect the vital interest of individuals, or to comply with a legal obligation). However, it is necessary to comply with national laws which may sometimes restrict these provisions.

Regarding the processing of mobile location data, the EDPB emphasizes in particular that public authorities should first seek to process these data in an anonymous manner and when it is not possible to only process anonymous data, Member States must introduce legislative measures to safeguard public security. An example of adequate safeguards would be to provide users of electronic communication services the right to a judicial remedy. Finally, the EDPB recalls that, in accordance with the principle of proportionality, the least intrusive solution should always be preferred.

For further information: Website EDPB

To be noted: Since March 6, 2020, several European Supervisory Authorities have also published recommendations on their websites with respect to the processing of personal data in the context of the fight against the COVID-19, sometimes adopting different approaches.

For more information: Austria | Belgium | Bulgaria | Czech Republic | Denmark | Finland | France | Germany | Hungria | Iceland | Ireland| Italia |Lithuania |Luxembourg | Norway | Poland | United Kingdom |Slovakia |Slovenia |Spain | Sweden |Switzerland

03/18/2020 – EDPS | Annual report 2019

On March 18, 2020, the European Data Protection Supervisor (EDPS) published its 2019 Annual Report.

This report presents the various activities conducted by the EDPS in 2019, which focused on consolidating the achievements of previous years, assessing the progress made and defining future priorities.

For more information: Website EDPS

03/04/2020 – Court of Justice of the European Union | Opinion | Advocate General | Consent

The Advocate General of the Court of Justice of the European Union, Maciej Szpunar, issued his Opinion in the case (Case C-61/19) between the Romanian Data Protection Supervisory Authority and the telecommunications provider Orange Romania.

In March 2018, the Romanian Supervisory Authority had imposed an administrative sanction against Orange Romania for having collected and kept copies of identity documents of its customers without their express consent. The authority noted that the company had concluded agreements for the provision of telecommunications services and copies of the identity documents were attached to them. These agreements would have stated that the customers had been informed and had given their consent to the collection and retention of these copies, as evidenced by the insertion of crosses in boxes added to the contractual clauses. However, according to the authority's findings, the company did not provide evidence that, at the time the agreements were concluded, the customers had an informed choice as to the collection and retention of these copies.

In that context, Orange Romania brought an action before the national court challenging the fine imposed on it. The latter referred two questions to the Court of Justice for a preliminary ruling. In his Opinion, the Advocate General suggests that the Court should reply that an individual who wishes to conclude an agreement *"for the provisions of telecommunication services with an undertaking does not give his or her 'consent', that is, does not indicate his or her 'specific and informed' and 'freely given' whishes, […] to that undertaking when he or she is required to state, in handwriting, on an otherwise standardized contract, that he or she refuses to consent to the photocopying and storage of his or her ID documents."*

For further information: Website IAPP | Curia

France

03/27/2020 – Council of State | Revocation of a decision from the French Supervisory Authority | Dereference | Google

On March 27, 2020, the Council of State revoked a decision of the French Supervisory Authority (the CNIL) concerning the geographical scope of the right to be forgotten.

On March 10, 2016, the CNIL had imposed a fine to Google for failing to comply with a formal notice issued by the CNIL to make effective the dereferencing on all national versions of its search engine Google Search. Google appealed against this decision before the Council of State which, in line with European Court of Justice's ruling of September 24, 2019, revoked the CNIL's decision.

In its decision, the Council of State emphasized that the alleged breach by Google must be ruled in accordance with the provisions of the French Data Protection Act No. 78-17 of January 6, 1978 as amended implementing the Directive of October 24, 1995, considering that the CNIL's sanction was issued in 2016. The Council of State also refers to the European principle of dereferencing and considers that, as the French legislator has not adopted any specific provisions allowing the CNIL to dereference beyond the scope of EU law, the CNIL can only order a European dereferencing.

For further information: Council of State's Decision | CNIL Website

---

03/25/2020 – French Supervisory Authority | Recommendation on cookies & other trackers | Postponement

The adoption of the final version of the draft recommendation on "Cookies & other trackers", initially scheduled for early April, is postponed.

On March 25, 2020, the French Supervisory Authority indicated in a publication on its website that the adoption of the final version of the draft recommendation on "Cookies and other trackers", initially scheduled for early April, is postponed to a later date, which will be set depending of the evolution of the health situation.

For further information : CNIL Website

03/12/2020 – French Supervisory Authority | Control Strategy 2020

In a statement dated March 12, 2020, the French Supervisory Authority (the CNIL) presents the topics on which it will focus in priority in 2020, i.e., health data, geolocation used in the context of local services and cookies and other trackers.

With regard to the security of health data, the CNIL is willing to focus on the security measures implemented by health professionals or on their behalf in order to protect these data which are subject to a specific protection under applicable regulations.

As to geolocation, the CNIL wants to increase its investigations on services whose purpose is to facilitate daily life by using location data (these investigations will focus in particular on the proportionality of the data collected in this context, the retention periods defined, the information provided to individuals and the security measures implemented).

Concerning cookies and other trackers, the CNIL specifies that the recommendation to guide operators will be published in the spring of 2020 (please note that this date has been postponed following the COVID-19 crisis). A period of 6 months to comply will then be given to the organizations from the publication of the final recommendation. Thus, the CNIL will start its investigations in autumn 2020.

For further information: CNIL Website

03/06/2020 – French Supervisory Authority | COVID-19 | Recommendations

In the context of the health crisis of the COVID-19, the French Supervisory Authority (the CNIL) reminded, on March 6, 2020, the principles relating to the collection of personal data, in particular focusing on the collection of health data by employers.

In its publication, the CNIL responds to solicitations from professionals and individuals on the question of the collection of personal data in order to determine if individuals have symptoms of COVID-19. On this occasion, it provides for "dos and don'ts".

As part of the "Don'ts", the CNIL provides that employers should refrain from collecting - in a systematic and generalized manner or through surveys or individual requests - information related to the research of potential symptoms presented by an employee/agent or his/her relatives. As an example, the CNIL specifies that it is not possible to implement a mandatory body temperature readings for each employee/agent/visitor to be sent daily to his/her superiors.

Nevertheless, the CNIL mentions the possibilities offered to employers, particularly under the French Labor Code and their responsibility for the health and safety of their employees. For example, the CNIL specifies that employers can raise awareness and invite their employees to provide individual feedback concerning them in relation to a possible exposure to the virus. In the event of a reporting, an employer is entitled to record the date and identity of the individual suspected of having been exposed and the organizational measures taken and then, communicate to the health authorities, upon request, the elements related to the nature of the exposure. The CNIL also specifies that, in application of the French Labor Code, each employee/agent is obliged to inform his or her employer in the event of suspected contact with the virus.

For further information: CNIL Website

Ireland

03/25/2020 – Irish Supervisory Authority | COVID-19 | Data Subject Access Requests

On March 25, 2020, the Irish Supervisory Authority (DPC) issued a guidance on the handling of data subjects' access requests in the context of COVID-19.

The authority states that it is aware of the difficulties created by the health crisis and recommends a methodology for responding to data subjects' requests. Any organization encountering difficulties in responding to requests should therefore, to the extent possible, communicate with individuals concerned about the processing of their request, including any extension of the response time. Furthermore, the DPC reminds that the GDPR provides for a two-month extension to respond to a request when necessary given the complexity and number of requests.

While it is not possible to derogate from the statutory obligations, the DPC specifies that if a complaint is filed, the facts of each case, including any mitigating circumstances specific to each organization, will be fully taken into account by the authority.

For further information: DPC Website

Italy

03/04/2020 – Italian Supervisory Authority | COVID-19 | Recommendations

The Italian Supervisory Authority published on its website recommendations on the processing of personal data in the context of the health crisis of COVID-19.

The Italian authority states that employers should not collect, in advance and in a systematic and generalized manner - including through specific requests to an employee or through surveys - information about the presence of symptoms or about their movements in a personal context. The authority reminds in this regard that the collection of information on the symptoms of COVID-19 and on the recent movements of each individual is the responsibility of health professionals and the civil protection system, which have to ensure compliance with public health rules.

However, the authority emphasizes that the employer may invite its employees to report if they went to a high-risk area, particularly since the employee has an obligation to inform his employer of any danger to health and safety in the workplace. Furthermore, the authority specifies that when an employee performing duties involving contact with the public encounters a suspected case of COVID-19 in the course of his/her work, he/she must ensure that the competent health services are informed - including through the employer - and must follow the preventive instructions provided by the health services consulted.

For further information: Website IAPP | Italian Supervisory Authority Website

---

Netherlands

03/03/2020 – Dutch Supervisory Authority | Fine | Sale of personal data

The Dutch Supervisory Authority imposed a fine of €525,000 on a tennis association for selling its members' personal data.

In 2018, the association illegally sold the personal data of a few thousand of its members to two sponsors, providing them with data such as name, gender and address, so that the sponsors could offer them tennis-related offers. The association appealed against the sanction, arguing that it had a legitimate interest in selling its members' data.

For further information: EDPB Website | Website IAPP

Poland

03/05/2020 – Polish Supervisory Authority | Fine | Biometric Data | Children

The Polish Supervisory Authority imposed an administrative fine of PLN 20,000 (less than €5,000) on a school for processing biometric data in a school canteen.

It has been established that the school used a biometric tool at the entrance of the school canteen to identify the children in order to verify the payment of meal prices. The authority pointed out that, in the context of this processing operation, the school processed special categories of personal data of 680 children without a legal basis when it had the possibility to use alternative forms of identification (e.g., electronic cards, names, contract numbers). In its decision, the authority ordered the deletion of the personal data processed in the form of digital information relating to the children's fingerprints and the cease of any further data collection.

For further information: EDPB Website | Polish Supervisory Authority Website

---

Spain

03/02/2020 – Spanish Supervisory Authority | Fines | Consent | Security Measures

On 27 and 28 February 2020, the Spanish Supervisory Authority imposed fines of a total amount of €168,000 on two Vodafone's subsidiaries for violation of the GDPR.

The subsidiary Vodafone España was fined for violating the provisions on consent of Articles 5 (1) and 6 (1) of the GDPR as it was unable to provide proof of its customers' consent to the processing of their personal data.

The second subsidiary, Vodafone ONO, was fined for failing to comply with the provisions of Article 32 of the GDPR relating to the implementation of appropriate technical and organizational measures to ensure data security.

For further information: Decision of the Spanish Supervisory Authority | Decision of the Spanish Supervisory Authority

---

Sweden

03/11/2020 – Swedish Supervisory Authority | Fine | Google | Right to request delisting

On March 11, 2020, the Swedish Supervisory Authority imposed a sanction of approximately 7 million euros on Google LLC for failure to comply with its obligations relating to the right to request delisting.

In 2017, the authority conducted an audit on how Google handles the individuals' right to request delisting on its search engine.

In its decision, the authority ordered Google to delete a number of search results. In 2018, the authority conducted a follow-up audit to verify that Google had complied with its first decision. On this occasion, the authority notably found that Google had not correctly deleted two of the search result lists that the authority had ordered to delete in 2017.

On the one hand, Google interpreted too narrowly the web addresses to be removed from the list of search results. On the other hand, Google did not delete the list of search results without undue delay. It is specified that when Google removes a link from the search results, it informs the website to which the link is directed. This then allows the website to republish the page in question on another link which will then be displayed in a Google search. In other words, the right to delisting has no practical effect.

The authority noted that Google does not have a legal basis for informing website owners when search result lists are removed and that, furthermore, the company gives misleading information to individuals about the effectiveness of their requests. Therefore, the authority ordered Google to cease this practice. Google may appeal against this decision within 3 weeks. If Google decides not to appeal, this decision will take effect at the end of that period.

For further information: EDPB Website

United Kingdom

03/04/2020 – UK Supervisory Authority | Fine | Personal Data Breach

The UK Information Commissioner's Office (ICO) has fined Cathay Pacific Airways Limited £500,000 for failing to protect the security of its customers' personal data.

Between October 2014 and May 2018, the computer systems of the company lacked appropriate security measures which led to customers' personal details being exposed, 111,578 of whom were from the UK, and approximately 9.4 million more worldwide. Due to the timing of these incidents, the ICO investigated this case under the Data Protection Act 1998.

Various errors were found during the ICO's investigation (e.g., back-up files that were not password protected; insufficient anti-virus protection), which constitute a breach to Principle 7 of the Data Protection Act 1998.

For further information: Website IAPP |ICO Website

03/02/2020 – UK Supervisory Authority | Fine | Automated Nuisance Calls

The UK Information Commissioner's Office (ICO) has fined CRDNN Limited with a £500,000 fine for making more than 193 million automated nuisance calls.

Following an investigation on computer equipment and documents in March 2018, the ICO investigation revealed that CRDNN Limited was found to be making nearly 1.6 million calls per day about window scrappage, debt management and window sales between 1 June and 1 October 2018. The calls were all made from fraudulent numbers, which meant that people who received the calls could not identify who was making them. The ICO considered that the company broke the law by not gaining consent from the phone owners to make those calls and by not providing a valid opt out.

For further information: ICO Website

Other News

03/31/2020 – Marriott | Personal Data Breach Notification

Marriott International announced that it has experienced another personal data breach.

The hotel chain stated that it discovered that guest information had been accessed using the login credentials of two employees. The incident was identified in February but was reported to have started in mid-January 2020. The compromised data included guest contact details, loyalty account information

and personal details such as date of birth and gender. Marriott International has set up an online portal for guests to determine whether their personal data were involved in the incident.

For further information: Website IAPP | Website Marriott International

---

03/26/2020 – – EDPS | European Commission | Location Data

According to an article published on Reuters, various telecom operators accepted to share their data with the European commission in the context of the fight against the virus.

The European Data Protection Supervisor (EDPS) has published on its website a letter addressed to the European Commission in this respect. In its letter, the EDPS clarified that, to the extent the data are effectively anonymized, the rules of the GDPR would not apply to the data shared by telecom operators. Having said that, the EDPS indicated that such effective anonymization requires more than simply removing obvious identifiers (such as phone numbers) and that it is necessary to ensure that indirect identification is not possible.

Besides, the EDPS specifies the importance of respecting the principle of transparency, ensuring the deletion of data in the aftermath of the crisis and ensuring a high level of data security, in particular by ensuring that these levels of security will be respected by the third parties on which the Commission will rely to process the information.

For further information: Website Reuters | Website de l'EDPS

03/22/2020 – Cyber-attack | AP-HP (French hospitals)

On March 22, 2020, the *Assistance Publique - Hôpitaux de Paris (AP-HP)* would have been the target of a cyber-attack (denial of service attack - DDoS).

For further information: Website Nextinpact

03/15/2020 – ENISA | Cybersecurity | Teleworking

In a publication dated March 15, 2020, the Director of the European Network and Information Security Agency (ENISA) shared his top tips for teleworking in times of COVID-19.

It is notably recommended to work with a secure Wi-Fi connection and regularly updated anti-virus systems, make periodic backups and have up to date security software. With respect to the actions that employers can take, it is recommended that they provide regular feedback to their employees on the procedure to follow in case of problems.

For further information: Website ENISA

03/10/2020 – Criteo | Privacy International | French Supervisory Authority Investigation

On March 10, 2020, various media announced that Criteo would be subject to an investigation by the French Supervisory Authority (the CNIL) following a complaint by the association Privacy International.

Criteo sent a press release to the media "Techcrunch" confirming that in January 2020, the CNIL opened an investigation in response to a complaint filed by Privacy International in November 2018. The CNIL being the competent supervisory authority for Criteo, the company states that this procedure is normal and that it had already disclosed such investigation in its annual review. In particular, the company states in the press release that it will cooperate with the CNIL in its investigation and that it remains confident in its privacy practices.

For further information: Website Techcrunch

This newsletter has been prepared by the Technology & Innovation team of the Paris office. For further information, you may contact us by email:

***Ahmed Baladi**, Partner - ABaladi@gibsondunn.com*
***Vera Lukic**, Of counsel - VLukic@gibsondunn.com*
***Adélaïde Cassanet**, Associate - ACassanet@gibsondunn.com*
***Guillaume Buhagiar**, Associate - Gbuhagiar@gibsondunn.com*
***Clémence Pugnet**, Associate - CPugnet@gibsondunn.com*