Monitoring Report – 11 /01/2019

Week in Review

efamro comments:

An interesting privacy opinion from Advocate General of the Court of Justice of the European Union (CJEU) marked the start of a new year in data protection and privacy. Is the scope of the right to be forgotten likely to be limited to EU domains only? The CJEU Advocate General opinion in a case between Google and CNIL found that geo-blocking was sufficient and that complete "de-referencing" from the search engine was not necessary. Although not binding, the CJEU generally follows lead of Advocate General.

On the EU-U.S. Privacy Shield, the Commission's second review noted that the framework showed improvements but a permanent Ombudsperson should be nominated by 28 February 2019.

EU regulators continue to investigate the activities of Cambridge Analytica and Facebook. The UK's Information Commissioner's Office (ICO) took some limited enforcement action against SCL (parent of Cambridge Analytica) which led to a fine of £15,000. This fine was levied for failure of the company to comply with a data subject access request from a citizen, outside the EU.

As uncertainty on the terms of the UK withdrawal from the EU rumbles on, organisations, particularly small research suppliers, making Brexit contingency plans for data flows between the EEA and the UK may find recent guidance issued by the UK ICO helpful. Additionally, the Department of Commerce has updated its frequently asked questions on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks to clarify the effect of the UK's planned withdrawal from the EU on March 29, 2019.

EU Data Protection – CJEU Opinion on Right to be Forgotten

Advocate General Szpunar proposes that the Court should limit the scope of the de-referencing that search engine operators are required to carry out to the EU (Press Release)

By decision of 21 May 2015, the President of the French Commission nationale de l'informatique et des libertés (National Commission for Information Technology and Civil Liberties; 'the CNIL') served formal notice on Google that, when acceding to a request from a natural person for the removal of links to web pages from the list of results displayed following a search performed on the basis of that person's name, it must apply that removal to all of its search engine's domain name extensions.

Google refused to comply with that formal notice, merely removing the links in question from only the results displayed following a search performed on the domain names corresponding to the versions of its search engine in the Member States of the EU. Moreover, the CNIL regarded as insufficient Google's further 'geo-blocking' proposal, made after the time limit laid down in the formal notice had passed, whereby internet users would be prevented from accessing the results in question, from an IP address deemed to be located in the State of residence of the person concerned, after performing a search on the basis of that person's name, no matter which version of the search engine they used. By adjudication of 10 March 2016, the CNIL, after finding that Google had failed to comply with that formal notice by the prescribed time limit, imposed on it a penalty, which was publicised, of €100 000. By an application lodged before the Conseil d'État (Council of State, France), Google seeks to have that adjudication annulled. The Conseil d'État decided to refer several questions to the Court of Justice for a preliminary ruling.

In today's Opinion, Advocate General Maciej Szpunar begins by indicating that the provisions of EU law applicable to the present case1 do not expressly govern the issue of the territorial scope of de-referencing. He therefore takes the view that a distinction must be made depending on the location from which the search is performed. Thus, search requests made outside the EU should not be affected by the de-referencing of the search results. He is therefore not in favour of giving the provisions of EU law such a broad interpretation that they would have effects beyond the borders of the 28 Member States. The Advocate General thus underlines that, even though extraterritorial effects are possible in certain, clearly defined, cases affecting the internal market, such as in competition law or trademark law, by the very nature of the internet, which is worldwide and found everywhere in the same way, that possibility is not comparable.

According to the Advocate General, the fundamental right to be forgotten must be balanced against other fundamental rights, such as the right to data protection and the right to privacy, as well as the legitimate public interest in accessing the information sought. The Advocate General continues that, if worldwide de-referencing were permitted, the EU authorities would not be able to define and determine a right to receive information, let alone balance it against the other fundamental rights to data protection and to privacy. This is all the more so since such a public interest in accessing information will necessarily vary from one third State to another depending on its geographic

location. There would be a risk, if worldwide de-referencing were possible, that persons in third States would be prevented from accessing information and, in turn, that third States would prevent persons in the EU Member States from accessing information.

However, the Advocate General does not rule out the possibility that, in certain situations, a search engine operator may be required to take de-referencing actions at the worldwide level, although he takes the view that the situation at issue in the present case does not justify this.
He therefore proposes that the Court should hold that the search engine operator is not required, when acceding to a request for de-referencing, to carry out that de-referencing on all the domain names of its search engine in such a way that the links in question no longer appear, irrespective of the location from which the search on the basis of the requesting party's name is performed.

However, the Advocate General underlines that, once a right to de-referencing within the EU has been established, the search engine operator must take every measure available to it to ensure full and effective de-referencing within the EU, including by use of the 'geo-blocking' technique, in respect of an IP address deemed to be located in one of the Member States, irrespective of the domain name used by the internet user who performs the search.

Advocate General Szpunar proposes that the Court should hold that the operator of a search engine must, as a matter of course, accede to a request for the de-referencing of sensitive data (Press Release)

The operator of a search engine must, however, ensure protection of the right of access to information and of the right of freedom of expression

A dispute has arisen between, on the one hand, Ms G.C., Mr A.F., Mr B.H. and Mr E.D. and, on the other hand, the Commission nationale de l'informatique et des libertés (French Data Protection Authority) ('the CNIL') with regard to four of that authority's decisions refusing to put the company Google Inc. on formal notice to de-reference various links, included in the results list displayed following a search made on the basis of their names, to web pages published by third parties. The web pages in question contain, inter alia, a satirical photomontage of a female politician posted online under a pseudonym, an article referring to one of the interested parties as the public relations officer for the Church of Scientology, the placing under investigation of a male politician and the conviction of another interested party for sexual assaults against minors.

After the interested parties had brought proceedings before it challenging the refusal of the CNIL to put Google on formal notice to carry out the 'de-referencing' requested, the Conseil d'État (Council of State) (France) referred several questions to the Court of Justice concerning the interpretation of the directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

By its first question, the Conseil d'État seeks to ascertain whether, having regard to the responsibilities, powers and specific capabilities of the operator of a search engine, the prohibition imposed on other data controllers on processing data falling within certain specific categories (such as

political opinions, religious or philosophical beliefs, sex life) is also applicable to such an operator. In his Opinion delivered today, Advocate General Maciej Szpunar begins by stating that the provisions of Directive 95/46 should be interpreted in such a way as to take account of the responsibilities, powers and capabilities of a search engine. Thus, he points out that the prohibitions and restrictions laid down by Directive 95/461 cannot apply to the operator of a search engine as if it had itself placed sensitive data on the web pages concerned. Since the activity of a search engine logically takes place only after (sensitive) data have been placed online, those prohibitions and restrictions can therefore apply to a search engine only by reason of that referencing and, thus, through subsequent verification, when a request for de-referencing is made by the person concerned.

The Advocate General accordingly proposes that the Court should find that the prohibition imposed on other data controllers on processing data falling within certain specific categories applies to the activities of the operator of a search engine.

The second question referred to the Court by the Conseil d'État asks whether an obligation is imposed on the operator of a search engine systematically to de-reference material. The Advocate General points out that Directive 95/46 lays down a prohibition on the processing of sensitive data.

Consequently, he states that the prohibition on the operator of a search engine processing sensitive data requires that operator to accede, as a matter of course, to requests for de-referencing relating to links to web pages on which such data appear, subject to the exceptions provided for by Directive 95/46.2 The Advocate General takes the view that the exceptions to the prohibition on the treatment of sensitive data, laid down by Directive 95/46, apply even though some of the exceptions appear to be more theoretical than practical as regards their application to a search engine.

The question of the derogations authorised under freedom of expression3 and their reconciliation with the right to respect for private life is then addressed by the Advocate General. He proposes that the Court should reply that, where there is a request for de-referencing relating to sensitive data, the operator of a search engine must weigh up, on the one hand, the right to respect for private life and the right to protection of data and, on the other hand, the right of the public to access the information concerned and the right to freedom of expression of the person who provided the information.

Lastly, the Advocate General addresses the question of the request for de-referencing relating to personal data which have become incomplete, inaccurate or obsolete, such as, for example, press articles relating to a period before the conclusion of judicial proceedings. The Advocate General proposes that the Court should hold that, in such circumstances, it is necessary for the operator of a search engine to conduct a balancing exercise on a case-by-case basis between, on the one hand, the right to respect for private life and the right to protection of data under Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union and, on the other hand, the right of the public to access the information concerned, while taking into account the fact that that information relates to journalism or constitutes artistic or literary expression.

EU-US Privacy Shield– Commission comments second review shows improvements but a permanent Ombudsperson should be nominated by 28 February 2019

EU-U.S. Privacy Shield: Second review shows improvements but a permanent Ombudsperson should be nominated by 28 February 2019

Press Release from the European Commission on the publication of the report on the second annual review of the functioning of the EU-U.S. Privacy Shield.

This year's report shows that the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the U.S. The steps taken by the U.S. authorities to implement the recommendations made by the Commission in last year's report have improved the functioning of the framework.

However, the Commission does expect the US authorities to nominate a permanent Ombudsperson by 28 February 2019 to replace the one that is currently acting. The Ombudsperson is an important mechanism that ensures complaints concerning access to personal data by U.S. authorities are addressed.

Andrus Ansip , Commission Vice-President for the Digital Single Market, said: " Today's review shows that the Privacy Shield is generally a success. More than 3,850 companies have been certified, including companies like Google, Microsoft and IBM – along with many SMEs. This provides an operational ground to continuously improve and strengthen the way the Privacy Shield works. We now expect our American partners to nominate the Ombudsperson on a permanent basis, so we can make sure that our EU-US relations in data protection are fully trustworthy."

Commissioner for Justice, Consumers and Gender Equality, **Věra Jourová** ,stated: " The EU and the U.S. are facing growing common challenges, when it comes to the protection of personal data, as shown by the Facebook / Cambridge Analytica scandal. The Privacy Shield is also a dialogue that in the long term should contribute to convergence of our systems, based on strong horizontal rights and independent, vigorous enforcement. Such convergence would ultimately strengthen the foundation on which the Privacy Shield is based. In the meantime, all elements of the Shield must be working at full speed, including the Ombudsperson. "

Improvements already made include the strengthening by the **Department of Commerce** of the certification process and of its proactive oversight over the framework. As recommended by the Commission's first annual review, the Department of Commerce has set up several mechanisms, such as a system of checks ("spot checks"), which randomly selects companies to verify that they comply with the Privacy Shield principles. 100 companies have been checked: 21 had issues that have now been solved. Additional compliance review procedures also include the analysis of Privacy Shield participants' websites to ensure that links to privacy policies are correct. The Department of

Commerce put in place a system to identify false claims which prevents companies from claiming their compliance with the Privacy Shield, when they have not been certified.

The **Federal Trade Commission** has also demonstrated a more proactive approach to enforcement by monitoring the principles of the Privacy Shield, including by issuing subpoenas to request information from the participating companies.

As regards access to personal data by U.S. public authorities for national security purposes, new members of the Privacy and Civil Liberties Oversight Board (PCLOB) have been appointed which restores the Board's quorum. The Board's report on the implementation of Presidential Policy-Directive No. 28 (PPD-28, which provides for privacy protections for non-Americans) has been made publicly available. It confirms that these privacy protections for non-Americans are implemented across the U.S. intelligence community.

The second review took into account relevant developments in the U.S. legal system in the area of privacy. The Department of Commerce launched a consultation on a federal approach to data privacy to which the Commission contributed and the US Federal Trade Commission is reflecting on its current powers in this area. In the context of the Facebook/Cambridge Analytica scandal, the Commission noted the Federal Trade Commission's confirmation that its investigation of this case is ongoing.

Next steps

The report will be sent to the European Parliament, the Council, the European Data Protection Board and to the U.S. authorities.

The European Commission expects the U.S. government to identify a nominee to fill the Ombudsperson position on a permanent basis by 28 February 2019 at the latest. If this does not take place by that date, the Commission will consider taking appropriate measures, in accordance with the General Data Protection Regulation.

Background

The EU-U.S. Privacy Shield decision was adopted on 12 July 2016 and the Privacy Shield framework became operational on 1 August 2016. It protects the fundamental rights of anyone in the EU whose personal data is transferred to certified companies in the United States for commercial purposes and brings legal clarity for businesses relying on transatlantic data transfers.

The Commission committed to reviewing the arrangement on an annual basis, to assess if it continues to ensure an adequate level of protection for personal data. After the first annual review, which took place in 2017, the Commission made a number of recommendations to further improve the practical functioning of the Privacy Shield.

On 18 October 2018, Commissioner for Justice, Consumers and Gender Equality Věra **Jourová** , launched with the US Secretary of Commerce Wilbur Ross the discussions for the second review

the EU-U.S. Privacy Shield (statement). The findings in this report are based on meetings with representatives of all US government departments in charge of running the Privacy Shield, including the Federal Trade Commission, the Office of the Director of National Intelligence (ODNI), the Department of Justice and the State Department, which took place in Brussels mid-October 2018, a study on automated decision-making commissioned by the Commission as well as on input from a wide range of stakeholders, including feedback from companies and privacy NGOs. Representatives of the EU's independent data protection authorities also participated in the review.

France General Data Protection Regulation (Guidance) – Data Sharing

Hunton Andrews Kurth reports that the French supervisory authority, the CNIL, has published guidance on data sharing with business partners or data brokers. On December 28, 2018, the CNIL published guidance regarding the conditions to be met by organizations in order to lawfully share personal data with business partners or other third parties, such as data brokers. The guidance focused, in particular, on such a scenario in the context of the EU General Data Protection Regulation ("GDPR"). The CNIL guidance sets forth the 5 following conditions:

- **Prior consent:** Organizations must seek the individual's consent prior to sharing personal data with the organization's partners.
- **Identification of the partners:** The data collection form must provide notice of the particular partner(s) who may receive the personal data. According to the CNIL guidance, the organization that first collects the data may either (1) publish an exhaustive and regularly updated list of partners directly on the data collection form, or (2) insert a link to that list on the form, together with a link to the partners' privacy policies.
- **Notification of changes to the list of partners:** Individuals must be informed of any updates to the list of partners and, in particular, of the fact that their personal data may be shared with new partners. This information may be provided on two "levels": (1) each marketing message sent by the organization that collects the data must provide an up-to-date list of partners (see above); and (2) each new partner receiving an individual's data must inform the individual, in its first communication to the data subject, of such processing. (See last bullet point below.)
- **Limit to further sharing without consent:** The partners may not share the personal data with their own partners without seeking the individual's informed consent.
- **Notice to be provided by the partners at the time of the first communication to the individual:** The partners who process the personal data to send their own marketing communications must inform the concerned individuals of the source from which the data originates (by providing the name of the organization who shared the data with them), and how the individuals may exercise their data protection rights, in particular, their right to object to the

processing of their personal data for direct marketing purposes. The CNIL guidance states that individuals may exercise their right to object either directly by contacting the partner, or by contacting the organization who first collected the data. That organization is required to pass the objection on to its partners who received that individual's data

Source: Hunton Andrews Kurth

URL: https://www.huntonprivacyblog.com/2019/01/02/cnil-publishes-guidance-on-data-sharing-with-business-partners-or-data-brokers/?mkt_tok=eyJpIjoiWW1RMk9EUTBORFpsTW1FNCIsInQiOiJiZFdrUVFDaVhrZzJZNlIyWjM0TDRhUVBsekhWTFc0YU05N3VXcjhYd3JIZ2VpOEtTVDltQlpDZ1pDaDJ0MlR5MXplbElFeFhiWmtqTnJOYlVhS1NyWlwvKzNLZERySFZqZmxjNkE3QVVnMkFlbk8xdXJSeHFNRjNcL1FtRFROdEl5Ino%3D

United Kingdom General Data Protection Regulation (Guidance) – Updated Guidance

The UK's supervisory authority the ICO has published new guidance and updated its existing data protection guidance in several areas including:

- published updated guide to data protection, which covers the Data Protection Act 2018 and the GDPR as it applies in the UK. The guide combines the existing ICO guides to the GDPR and Law Enforcement Processing, with the addition of new pages on intelligence services processing and key data protection themes.
- reviewed its guidance on Data Protection Impact Assessments (DPIAs) under the GDPR to reflect the opinions from the European Data Protection Board (EDPB). The updated guidance includes the published list of processing operations likely to result in high risk and also provides more advice on how to assess whether your intended use of personal data requires a DPIA.
- expanded its guidance on contracts, published guidance on controllers and processors and published detailed guidance on controllers and processors and contracts and liabilities.

Source: ICO

URL: www.ico.org..uk

UK Data Protection – Data Flows after Brexit (UK Guidance)

The ICO has published additional guidance data protection in the absence of an EU-UK Brexit deal for organisations that receive personal data from the European Economic Area (EEA) or operate in the EEA and send personal data outside the UK.

Source: ICO

URL: https://ico.org.uk/for-organisations/data-protection-and-brexit/

UK Data Protection – Data Flows after Brexit (Department of Commerce Guidance)

Hunton Andrews Kurth reports on the update of the Department of Commerce to the Privacy Shields to clarify the applicability to UK Personal Data. On December 20, 2018, the Department of Commerce updated its frequently asked questions ("FAQs") on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks (collectively, the "Privacy Shield") to clarify the effect of the UK's planned withdrawal from the EU on March 29, 2019.

The FAQs provide information on the steps Privacy Shield participants must take to receive personal data from the UK in reliance on the Privacy Shield after Brexit. The deadline for implementing the steps identified in the FAQs depends on whether the UK and EU are able to finalize an agreement for the UK's withdrawal from the EU. To the extent the UK and EU reach an agreement regarding withdrawal, thereby implementing a Transition Period in which EU data protection law will continue to apply to the UK, Privacy Shield participants will have until December 31, 2020, to implement the relevant changes to their public-facing Privacy Shield commitments described in the FAQs and below. To the extent no such agreement is reached, participants must implement the changes by March 29, 2019.

According to the FAQs, a Privacy Shield participant who would like to continue to receive personal data from the UK following the relevant deadline (as described above) must update any language regarding its public commitment to comply with the Privacy Shield to include an affirmative statement that its commitment under the Privacy Shield will extend to personal data received from the UK in reliance on the Privacy Shield. In addition, Privacy Shield participants who plan to receive Human Resources ("HR") data from the UK in reliance on the Privacy Shield must also update their HR Privacy Policies. The FAQs further state that if a Privacy Shield participant opts to make such public commitments to continue receiving UK personal data in reliance on the Privacy Shield, the

participant will be required to cooperate and comply with the UK Information Commissioner's Office with regard to any such personal data received.

Source: Hunton Andrews Kurth

URL: https://www.huntonprivacyblog.com/2018/12/26/department-of-commerce-updates-privacy-shield-faqs-to-clarify-applicability-to-uk-personal-data/?mkt_tok=eyJpIjoiTXpabU9EZzRZV0UwT0RRNSIsInQiOiJFdzg4TVFZRUQyelYxWldySWhTNDZ5RGJCWHE2UnpTVUNBYkJxREpNMUFhSGZMd1RKN2hrSGp0UldhOFdzR05kaERxM3F2NkVOWnoyMDNiSUx6U0JyaGRiUWY3bGIrTW4wOERJVDVCcytseWtkQUxWN2M3cEpBOTdBc2JURXFjVyJ9

Upcoming Events

January 2019

CPPD 2019 Data Protection and Democracy

30 January to 1st February 2019, Brussels, Belgium

CPDP is an annual three-day conference devoted to privacy and data protection. The overarching theme of the 2019 edition is "Data Protection and Democracy". The entwinement between data analytics and democratic processes has been on the spotlight for the better part of the past two years.

URL: https://www.cpdpconferences.org/call-for-papers

March 2019

Forum Europe - 9th Annual European Data Protection and Privacy Conference

20 March 2019, Brussels, Belgium

The Annual European Data Protection and Privacy Conference will return to Brussels in Spring 2019. Gathering over 200 cross-sector delegates and attracting an impressive line-up of top-level speakers every year, this event has become the must-attend annual data protection and privacy conference held in Brussels.

We are delighted to announce that Commissioners Věra Jourová and Mariya Gabriel will join us as a keynote speakers at the event.

2018 was a pivotal year for data protection and privacy in both the EU and globally. The 9th European Data Protection and Privacy Conference will explore how the power of data can truly be harnessed through trust and responsible use, in order to deliver economic growth and societal benefits.

It will also debate how an international system based on shared principles and ethics might be developed – all in the context of increasing technological innovation, on-going regulatory discussions in the EU around digital evidence and ePrivacy, and other global political developments that either distract from or give focus to such developments.

- Conference Programme & Speakers
- Registration