MONITORING REPORT

N. 23/2019

IN THIS ISSUE

GDPR IN THE EYES OF THE MEMBER STATES

IN VIEW OF THE UPCOMING REVIEW OF GDPR, MEMBER STATES SUBMIT OBSERVATIONS CONCERNING THE APPLICATION OF VARIOUS PROVISIONS OF THE GDPR

Müge Fazlioglu for IAPP

The full comments are available here

Council of the European Union

Article 97 instructs the European Commission, by May 25, 2020, and once again every four years thereafter, to "submit a report on the evaluation and review of this Regulation to the European Parliament and the Council." At a minimum, these reports should examine "the application and functioning" of Chapter 4 on transfers of personal data to third countries or international organizations and Chapter 7 on cooperation and consistency mechanisms. What makes this review process so critical is that it may serve as an impetus for the commission to "submit appropriate proposals to amend" the GDPR.

Member states submitted comments pointing to the uncertainty, confusion and fragmentation that persists around the GDPR's application. For its part, Germany admitted that "some businesses and government agencies have said they feel overwhelmed following the GDPR's entry into application," while "[s]ome users have felt considerable uncertainty [and] been very confused" by seemingly new instruments created by the GDPR, such as records of processing activities and data protection officers.

To alleviate some of these ambiguities, the Czech Republic suggested that real cases of best practice, as well as cases of bad practice, could be published online for the benefit of other member states. It pointed to several issues in which best practices are needed, including conflict of interests of DPOs, professional qualifications of DPOs, the roles of controller and processor, transparency obligations to data subjects where data has been obtained from public sources, and additional identification pursuant to Article 11.

One of the biggest areas in which fragmentation has affected GDPR implementation has been in the protection of children's data. Namely, Ireland described the GDPR's approach to the protection of children as "fragmented and disjointed." While references to protections for children can be found in various recitals (38, 58, 65, 71, and 75) and articles (6.1(f), 8, 12, 40, and 57), they are like "a jigsaw puzzle" and "do not provide a coherent picture." France also pointed out that children's consent in Article 8, which leaves discretion to member states regarding the age of consent of minors, "is likely to cause implementation difficulties" and that assessing whether this needs to be revised should be a priority. In a similar vein, the Netherlands pushed for "only one uniform age of consent" to apply throughout the entire EU, as the current situation "leads to a problematic lack of legal certainty for all parties concerned; parents, children and controllers alike."

Furthermore, the Czech Republic noted that, if the European Data Protection Board were to issue its own, even non-exhaustive, list of processing operations subject to or exempted from impact assessments, it would "contribute to much more uniform and consistent application of the GDPR." Germany also urged DPAs to harmonize their practice of interpretation more closely regarding risky processing operations and data protection impact assessments.

Member states made numerous comments about the effectiveness of and expectations placed upon supervisory authorities. On the bright side, member states drew attention to the effectiveness of the cooperation efforts between SAs. Latvia, for example, noted that several complaints by data subjects have been resolved successfully through the cooperation of the Latvian and Lithuanian SAs.

Others, meanwhile, focused on the shortcomings in the work done by SAs. For example, Germany noted that businesses would like "faster and more concrete assistance from the data protection authorities," while "[d]ata subjects would like more advice and faster processing of their requests." Germany also asked for transparent criteria for SAs regarding the issuance of fines "in order to ensure comparability and uniform enforcement." France called for "national disparities which hinder cooperation for supervisory authorities" to be "examined and removed."

Lithuania raised a question as to whether an appeal judgment in a national court in one jurisdiction would be legally binding on the lead SA in another jurisdiction.

Finding that a large number of data subjects make complaints to SAs after they are notified of a data breach via Article 33, Bulgaria stated that "difficulties arise in handling complaints on the same issue." Bulgaria noted that "the obligation to handle complaints [vis-à-vis Article 77] itself obstructs the work of the data protection authority." Bulgaria also noted that while Article 57, Paragraph 4 considered the excessiveness of a request to the SA is hinged on the repetitiveness of requests arising from a single data subject, it does not consider excessiveness in the sense of "multiple identical requests made by a large number of data subjects … regarding the same case." Germany also pointed out that "data protection authorities are most likely overwhelmed by the massive volume of reports" in accordance with Article 33, of which there were 89,000 in the EU by April 2019.

Transfers of personal data

Most member states that commented on adequacy decisions offered positive reflections. Yet, a common criticism was that they "remain underused."

To address this problem, Germany urged the commission to "keep up its efforts to bring about additional adequacy decisions and to expand the existing ones to additional areas and sectors." The Netherlands submitted a list of countries, suggested by Dutch trade organizations, as potential future candidates for an adequacy finding. These included Singapore, Colombia, Mexico, South Africa, Serbia and Dubai International Financial Centre, as well as all countries that have ratified and implemented the modernized Convention 108+.

Regarding codes of conduct, Belgium explained that "there is a clear interest from various stakeholders to make use" of them, but there is a reluctance to do so "due to a lack of clear guidelines." Bulgaria referred to codes of conduct as "an extremely useful and practically oriented voluntary accountability tool" but one that is "widely regarded as a form of indulgence that impedes the powers of the supervisory authority." The Netherlands cast doubt on the validity of the interpretation of codes of conduct provided in the EDPB's recently adopted guidelines, arguing that the text of the GDPR should be clarified on this topic. In addition, the Netherlands stated that the institution of a monitoring body for codes of conduct should be optional, as it would likely act as a disincentive by introducing additional costs into the process.

Lithuania remarked that Recital 81 states standard contractual clauses may be adopted by SAs only after approval by the commission, a situation that "creates legal uncertainty as to the mandatory nature of such procedure." To remedy this, Lithuania recommended to consider whether this power of the commission be explicitly included in Article 28(8).

Finally, on binding corporate rules, "while a useful and necessary subsidiary mechanism," Belgium argued that their use "also runs counter to the harmonization objectives of the GDPR."

What's next?

To recap, Article 97(4) of the GDPR requires the commission to "take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources" while conducting its evaluation and review of the GDPR. In particular, the Council expects the Commission to request information from the Member States on three issues:

- the use of adequacy decisions;
- the independence and resources of DPAs, including about "their capacity to exercise their powers provided by the GDPR and to comply with their obligations in the context [of] the cooperation and consistency mechanisms"; and
- verification of the effectiveness of the "coherent interpretation and application of the GDPR throughout the EU by the cooperation and consistency mechanism provided by the GDPR."

EDPB PUBLISHES GUIDELINES FOR THE DATA PROCESSING RELATED TO CONTRACTS FOR ONLINE SERVICES IN THE CONTEXT OF ARTICLE 6(1)(B) OF GDPR

The EDPB adopted a final version of the guidelines on the scope and application of Article 6(1)(b) GDPR in the context of information society services. Following public consultation, points of clarification were included in the text. In its guidelines, the Board makes general observations regarding data protection principles and the interaction of Article 6(1)(b) with other lawful bases. In addition, the guidelines contain guidance on the applicability of Article 6(1)(b) in case of bundling of separate services and termination of contract.

They are available here

ITALIAN SUPREME COURT RULES ON DATA MINIMIZATION AND GDPR

The Supreme Court addressed a case in which Deutsche Bank S.p.A. included a clause in the contract for which, in the absence of the consumer's consent to the processing of their sensitive data, it would have stopped the provision of its services and operations.

The Court underlined that the clause by which the bank has subordinated the execution of its operations to the consent to the processing of sensitive data undoubtedly contrasts with the guiding principles of privacy law, which cannot be waived by private contractual autonomy. These principles concern the protection of general interests, moral and social values and fundamental rights and freedoms.
Among the principles that govern privacy protection is data minimization: using only indispensable data, pertinent and limited to what is necessary for the pursuit of the purposes for which they are collected and processed.
The bank has apodictically justified the need for mandatory client consent to process sensitive data with its own corporate "policy": an unspecified improvement of customer relations. More crucially, the bank has acknowledged that it does not need such data to operate.

It is therefore clear that the precautionary measure of requesting customers' consent to process sensitive data on the (somewhat remote) possibility that the Bank may become aware of them during its activity assumes the connotation of a mere pretext.

So, if the only intent of the bank was to provide for the mere cancellation and destruction of the sensitive data which it might have come to know purely by chance, it would not have been necessary to impose the prior and generic consent to their "treatment". The bank could have requested a one-time consent to the destruction and deletion of such data, once the need arose.

Italian poetry translated and frustrated by me, please get in touch if you want to know more.
Full ruling available here, in Italian

THE CALIFORNIA ATTORNEY GENERAL RELEASES THE TEXT OF THE PROPOSED REGULATIONS TO IMPLEMENT THE CALIFORNIA CONSUMER PRIVACY ACT.

The proposed regulations focus on five areas: notice, handling requests, identify verification, rules regarding minors and financial incentives. While CCPA implementation efforts such as these move forward, the law continues to receive pushback from spokespeople in industry and trade groups, which are planning to continue "to make every effort to move [federal legislation] as far and as fast we can."

NATIONAL DPAs GUIDANCE

SPANISH AEPD RELEASES PRIVACY BY DESIGN GUIDELINES

The Spanish Agency for Data Protection has released **"PRIVACY GUIDE FROM THE DESIGN"** guidelines to incorporate data protection principles and privacy requirements into new products or services from conception, CEPYME News reports. The document is divided into nine sections, including defining the foundational principles of PbD and privacy engineering, as well as different strategies for the practice. The guide notes "establishing a framework that guarantees data protection does not represent an obstacle to innovation, but rather offers advantages and opportunities for ... organizations, market and society as a whole." (Original articles are in Spanish.)

Full report is available here

Full guidance available here

ENFORCEMENT

GERMAN DPAS RELEASE GDPR FINING GUIDELINES

THE PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE IMPOSED A FINE OF AN AMOUNT HIGHER THAN PLN 2.8 MILLION (CA. 645,000 EUROS) ON MORELE.NET.

Germany's Data Protection Conference, Datenschutzkonferenz, has announced it published guidelines for the country's new EU General Data Protection Regulation fine regime. Latham & Watkins' Partner Tim Wybitul, CIPP/E, wrote the guidelines will help make fines more "consistent and predictable" while fines will be higher, with larger organizations subject to steeper penalties. Wybitul adds that DSK will seek to have the European Data Protection Board adopt the new fine regime for all EU member states. (Articles are in German.)

ICO LOOKS AT CONSIDERATIONS FOR USING AI TO FULFIL DSARS

As part of its ongoing call for input for its framework for auditing artificial intelligence, the U.K. Information Commissioner's Office looks at the challenges organizations may face as they craft AI systems designed to help fulfil data subject access requests. ICO Research Fellow in Artificial Intelligence Reuben Binns writes about the use of AI systems for access, erasure and rectification requests under the EU General Data Protection Regulation and where potential exemptions may pop up. Meanwhile, ICO Executive Director for Technology Policy Simon McDougall offers his takeaways from the recently concluded TechSprint event hosted by the Financial Conduct Authority. **Full Story**

IRISH DATA PROTECTION COMMISSION STATEMENT ON INCREASED FUNDING OF €1.6 MILLION IN 2020 BUDGET

The Data Protection Commission (DPC) has acknowledged the additional funding of €1.6 million allocated to the regulator, announced by the Government in Budget 2020. The increase in funding for 2020 brings the total funding allocation for the DPC to €16.9 million, representing an 11% increase on the 2019 allocation.

The Commissioner for Data Protection, Helen Dixon, in commenting on the funding received acknowledged the Brexit challenges in this Budget but stated that, "the DPC is disappointed that the additional funding allocated is less than one third of the funding that the DPC requested in its budget submission. The submission reflected a year of experience of regulating under the General Data Protection Regulation (GDPR) and highlighted the increased volumes and complexities involved. The DPC must now reassess its planned expenditure for 2020, particularly in relation to foreseen "non-pay" expenditure for which the DPC has received a zero increase in allocation."

Since the application of the GDPR on 25 May 2018, the DPC has seen a significant increase in workload. Since 1 January 2019, over 7,000 complaints and almost 5,000 breach notifications have been received. The office has been contacted by members of the public and organisations seeking guidance over 40,000 times in the same period.

Increases in funding in recent years have allowed the DPC to recruit additional staff with various specialist backgrounds towards meeting the demands of the tasks assigned under the GDPR, bringing staffing levels to 138 at present. This funding was critical given the low base from which the DPC started in 2015 to prepare for the new EU

regulation which includes the Irish DPC acting as EU lead supervisory authority in respect of the many global technology multinationals with European headquarters in Ireland. This lead EU regulatory role places the DPC at the front line of global data protection regulation.

HELLENIC DPA

ADMINISTRATIVE FINES IMPOSED ON A TELEPHONE SERVICE PROVIDER

(1) Imposition of a fine for breach of the principle of accuracy and data protection by design when keeping personal data of subscribers

The Hellenic DPA has received complaints from telephone subscribers of the Hellenic Telecommunications Organization ("OTE") who, although registered in the OTE's do-not-call register (according to Article 11 of Law 3471/2006), they received unsolicited calls from third companies for the promotion of products and services.

The investigation of the case showed that those subscribers had submitted a portability request for the transfer of their subscription to another provider. As a consequence, OTE deleted their entries from the do-not-call register. However, when those subscribers cancelled their portability request, there was no proper procedure to cancel their removal from the register. Subscribers were listed as registrants in the internal system of the provider's customer service, but their telephone numbers were not included in the register sent by OTE to the advertisers, as the two systems, due to the error in their interconnection, did not have the same content.

The Authority found that this incident affected a large number of individual subscribers, as there was an infringement of Article 25 (data protection by design) and Article 5 (1) (c) (principle of accuracy) of the General Data Protection Regulation (GDPR). It therefore imposed an administrative fine of EUR 200.000 on the basis of the criteria laid down in Article 83 (2) of the Regulation.

(2) Imposition of a fine for failure to satisfy the right to object and the principle of data protection by design when keeping personal data of subscribers

The Hellenic DPA has received complaints from the recipients of advertising messages from OTE concerning their lack of ability to unsubscribe from the list of recipients of advertising messages. In the course of the examination of the complaints it emerged that from 2013 onwards, due to a technical error, the removal from the lists of recipients of advertising messages did not operate for those recipients who used the "unsubscribe" link. OTE did not have the appropriate organizational measure, i.e. a defined procedure by which it could detect that the data subject's right to object could not be satisfied.

Subsequently, OTE removed around 8.000 persons from the addressees of the messages, who had unsuccessfully attempted to withdraw from 2013 onwards. The Authority has found an infringement of the right to object to the processing for direct marketing purposes (Article 21 (3) of the GDPR) as well as Article 25 (data protection by design) of the GDPR and imposed an administrative fine of EUR 200.000 on the basis of the criteria of Article 83 (2) of the Regulation.

Decision 34/2019 and Decision 31/2019 are available in Greek on www.dpa.gr "Decisions"

PRIVACY V. PUBLIC ORDER: HONG KONG'S DPA SEEKS BALANCED RESPONSE TO BAN ON FACE COVERING

The violent actions on the streets of Hong Kong have led to a government regulation banning the use of face masks starting on Sunday, 6 October. On 4 October, the office of the Privacy Commissioner for Personal Data (PCPD) gave the following response:

1. "While the prohibition on face covering would expose the faces of individuals, without the video recording of facial information it does not constitute collection of "Personal Data" under Personal Data (Privacy) Ordinance (Ordinance). Hence the prohibition on face covering during protests is not … contrary to the Ordinance."

2. "Personal privacy right is a fundamental human right, and has long been protected by the laws of Hong Kong. It was said that one's privacy might be constrained upon the enactment of [the] Prohibition on Face Covering Regulation. However, personal privacy right is not an absolute right, and is subject to legal restrictions, with the important considerations including public interest."

3. "While exercising personal privacy rights, balance must be struck with public interest, with the consideration of both the protection of personal data privacy and the interests of society at large, including public order and national security."

4. "In order to promptly and effectively detect a crime, … seriously improper conduct, dishonesty or malpractice, and with the consideration to apprehend, prosecute or detain an offender, the personal data privacy right of the offender will not override the interests of society at large. A person offending the law cannot take privacy as a "refuge" or "sanctuary" of his wrongdoings."

5. "If government or law enforcement agencies are involved in collection of personal data (such as video recording of members of the public in protests), they must comply with requirements of the Ordinance in control of the collection, holding, processing or use (including disclosure and transfer) of personal data."

PL&B Comment: The question arises whether Hong Kong police and security forces are able, once they have video footage of (unmasked) protestors, to subject it to facial recognition software (and any accessible databases, particularly the HK ID card), so as to identify protestors en masse, without the need for individual warrants.

EU-U.S. PRIVACY SHIELD

THIRD REVIEW WELCOMES PROGRESS WHILE IDENTIFYING STEPS FOR IMPROVEMENT

The European Commission published its report on the third annual review of the functioning of the EU-U.S. Privacy Shield. The report confirms 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. Since the second annual review, there have been a number of improvements in the functioning of the framework, as well as appointments to key oversight and redress bodies, such as the Privacy Shield Ombudsperson. Being in the third year of the Shield's operation, the review focused on the lessons learnt from its practical implementation and day-to-day functionality. Today there are about 5,000 companies participating in this EU-U.S. data protection framework.

Among the improvements, the third review notes that the U.S. Department of Commerce is ensuring the necessary oversight in a more systematic manner by, for example, carrying out monthly checks of a sample of companies to verify compliance with Privacy Shield principles.

Enforcement action has improved with the Federal Trade Commission taking enforcement action related to the Privacy Shield in seven cases.

An increasing number of EU individuals are making use of their rights under the Privacy Shield and the relevant redress mechanisms are functioning well.

In addition to the appointment of the permanent Ombudsperson, the final two vacancies on the Privacy and Civil Liberties Oversight Board have been filled, ensuring that it is fully-staffed for the first time since 2016.

However, the Commission recommends that certain concrete steps be taken to better ensure the effective functioning of the Privacy Shield in practice. This includes further strengthening the (re)certification process for companies who want to participate by shortening the time of the (re)certification process; expanding compliance checks, including concerning false claims of participation in the framework; and developing additional guidance for companies related to human resources data. The Commission also expects the Federal Trade Commission to further step up its investigations into compliance with substantive requirements of the Privacy Shield and provide the Commission and the EU data protection authorities with information on ongoing investigations.

Background

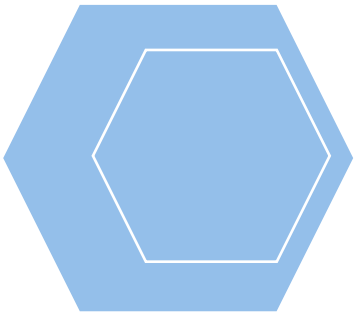
The EU-U.S. Privacy Shield decision was adopted on 12 July 2016 and the Privacy Shield framework became operational on 1 August 2016. It protects the fundamental rights of anyone in the EU whose personal data is transferred to certified companies in the United States for commercial purposes and brings 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. The first and second annual review took place in September 2017 and October 2018, respectively.

On 12 September 2019, the Director-General for Justice, Consumers and Gender Equality, Tiina Astola, and the U.S. Secretary of Commerce, Wilbur Ross, launched the discussions for the third review of the EU-U.S. Privacy Shield (statement). The findings in this report are based on meetings with representatives of all U.S. government departments in charge of running the Privacy Shield, including the Department of Commerce, the Federal Trade Commission, the Office of the Director of National Intelligence and the Department of Justice, which took place in Washington in September 2019, 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. There is currently litigation pending before the Court of Justice of the European Union on EU-U.S. data transfers, which may also have an impact on the Privacy Shield. A hearing took place in July 2019 in case C-311/18 (*Schrems II*) and, once the Court's judgement is issued, the Commission will assess its consequences for the Privacy Shield.

For More Information

- Report on the third annual review of the EU-U.S. Privacy Shield
- EU-U.S. Joint Statement from the third annual review



HOW TO 'BACKGROUND CHECK' UNDER THE GDPR

PIOTR FOITZICK FOR IAPP.

Information security, risk and compliance are in focus and one of the core issues for many companies. For obvious reasons it has been early recognized that people are one of the key factors and often times the weakest link in organizational security. From this point of view, it was natural to conclude that by knowing more about your employees and future employees you mitigate, to a degree, risks arising from internal threats, and you are employing people with proven records and sufficient level of integrity and trustworthiness.

Over time, this has become one of the security controls and something expected by your business partners and clients when analyzing your security or defining security requirements for potential vendors. Initially, minimizing the collection of personal data was not considered a key factor in this process, and there was little research on effectiveness of the different techniques, methods and types of information being utilized.

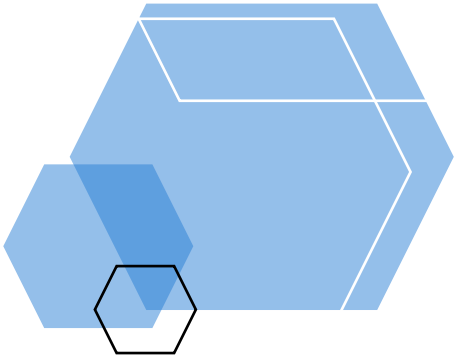
What is the GDPR perspective and what are the key issues?

Full article available here.

RESEARCHERS ROLLING OUT PRIVACY-PRESERVING AI LEARNING SYSTEM FOR MEDICAL ANALYSIS

ZDNet reports artificial intelligence researchers from big tech company Nvidia and King's College London will debut a new federated learning system that will allow doctors to collaborate on cases without sharing patient data. The new system will help neural networks function on decentralized data that follows an algorithmic model at different locations. The anonymized data is created through partial system contributions from network participants and the injection of white noise.

Full Story



DATA PROTECTION REPRESENTATIVE "CLASS" ACTION GETS THE GO AHEAD

It is alleged that Google tracked, surreptitiously, some of the internet activity of those users, so infringing rights protected by data protection legislation. The litigation is interesting for two reasons: it shows that you can claim damages under data protection legislation without proving any financial loss or even distress; and, it considers what is required for a representative action to be brought for this claim: Lloyd v Google LLC [2019] EWCA Civ 1599

Jason Rix for Allen & Overy

CHINESE CITIZENS WILL SOON NEED TO SCAN THEIR FACE BEFORE THEY CAN ACCESS INTERNET SERVICES OR GET A NEW PHONE NUMBER

China's 854 million internet users will soon need to use facial identification in order to apply for new internet or mobile services.

The Chinese government announced last month that telecommunications companies will need to scan users' faces in order to verify their identities before they can access new services.

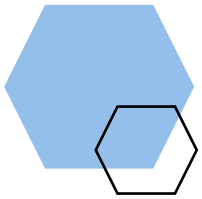
The new legislation is part of China's wider efforts to keep close tabs on its citizens and monitor their activities and behaviours.

Full story on Business Insider

PADDLING THE DATA LAKE

Bethan Blakeley shares her guide for not being overwhelmed by your data, and instead analyzing it with confidence and purpose.

IMPACT available here




efamro