ANNUAL PRIVACY FORUM 2021 - NOTES

1. INTRODUCTION

The value of personal data in the online world has significantly increased over the last years as electronic products, services and processes have permeated every fold of everyday life. Limitations in the transparency, the functionality and interconnectivity of online and communication services increases the risk of having personal data processed out of control of any accountable person or organization or simply becoming exposed to all sorts of privacy threats.

The EU legal framework on personal data protection is key in an effort to better control the processing of personal data while ensuring an adequate level of protection. Even the best legislative efforts cannot keep up to speed with the pace of innovative technology and business models that challenge the way personal data is processed and privacy is protected across the EU and beyond; therefore, examining what is at stake and where threats thereto originate from becomes of paramount importance.

Against this background, ENISA, DG CONNECT and the University of Oslo organized the Annual Privacy Forum (APF) 2021.

Due to the COVID-19 pandemic, this edition of APF, which was the ninth since 2012, was the second in a row that took place as an online event on the 17th and 18th of June 2021.

After a thorough peer-reviewing process, on the basis of significance, novelty and scientific quality 9 papers were selected (a 21% acceptance rate) and presented during the conference. These papers were organized across three thematic areas, were presented in three respective paper sessions and are available in the Conference Proceedings[1] published by Springer in the LNCS series.

This document presents, in brief, the key points made during the conference and relevant conclusions, complementing the published proceedings.

[1] https://link.springer.com/book/10.1007/978-3-030-76663-4

2. DAY 1 – JUNE 17, 2021

2.1 OPENING REMARKS

Evangelos Ouzounis, head of ENISA's Policy Development and Implementation Unit, welcomed the participants and opened the conference, introducing the motto of the event "Bringing Research and Policy Together" and thanking the co-organizers of the 2021 edition.

Nils Gruschka, Associate Professor at the University of Oslo followed, presented some of Oslo's landmarks, virtually transporting the participants to the Norwegian capital. Dr. Gruschka introduced Stephan Oepen, the head of the Informatics Department of the University of Oslo that is hosted in one of the largest computer science buildings in northern Europe and is named after Ole-Johan Dahl, one of the two inventors of Object Oriented Programming.

Prof. Oepen emphasized the importance of balancing technological development and societal needs taking into account privacy considerations, briefly presenting the example of the Norwegian Covid-19 contact tracing app, which was initially suspended by the country's DPA, due to privacy concerns. He then briefly presented the department's initiatives and research groups, including research groups on privacy and information security, which are among the areas of strategic investment for the university.

2.2 KEYNOTE TALKS

Bjørn Erik Thon the Commissioner and general director of Datatilsynet, the Norwegian DPA was the first keynote speaker. He elaborated on the case of the Norwegian covid-19 contact tracing app that was mentioned in the introduction explaining that Datatilsynet acts as an advisor but also as an inspection body. In the initial phases, they acted as advisors, to the ministry and the developers. After the launch of the app, they initiated an investigation, which turned into a big public discussion involving human rights protection where politicians were involved and even Amnesty International. The EDPB's opinion confirmed that the use of GPS for contact tracing was not appropriate and finally Datatilsynet issued a decision for the temporary ban of the processing in the beginning of June 2020, right in the middle of the pandemic. The public health authority reacted in compliance, by scrapping and deleting all collected data, given also that the usefulness of the app was not proven, due to very low adoption rates. A new app was designed in Norway and it was ready around Christmas time. He also confirmed that right now there's no open case concerning the new app. Next, Bjørn Erik Thon briefly presented the regulatory sandbox project, an initiative of Datatilsynet. It is a test environment where enterprises and public bodies can try new non-profit and innovative products, technologies and services closely followed by the DPA technologists and lawyers, promoting privacy friendly digitalization and development and especially Privacy by Design, even in areas such as machine learning and artificial intelligence. The sandbox received 25 high quality applications and four of them were chosen at the beginning of its operation on January 2021. He stated that he's confident that this project will prove to be a great success and that innovation and data protection can go hand in hand.

Final text pending approval by the speaker.

Aleid Wolfsen, deputy chair of the EDPB and chairman of the Dutch DPA, presented a concrete overview of the debates that the EDPB and EU/EEA DPAs are currently engaged in. He explained, that the EDPB is committed to support the co-legislators especially in relation to the rights to privacy and the protection of personal data. The EDPB and the EDPS are currently preparing their joint opinion on the proposed Artificial Intelligence Regulation**Error! Bookmark not defined.**. He stated that both institutions will emphasize that the AI Regulation should be aligned with the existing EU legislative framework including EU data protection rules, since the GDPR rules are applicable as long as there is personal data processing, even in AI. Another recent policy initiative which impacts the EU data protection framework is the proposed Data Governance Act that entails significant inconsistencies with the GDPR, in particular with regards to definitions and terminology, the need for legitimate legal basis, transparency and appropriate safeguards for the enforcement of these rules. He stated that data reuse, sharing and availability may generate benefits, but entail risks to the fundamental rights of individuals. So, data protection principles must be implemented from the early design stages of data processing. For the e-Privacy Regulation, he also stated that according to the EDPBs view[2], the review of the regulation has taken too long and it is high time to provide legal certainty for all stakeholders. It is vital that the future regulation does not lower the level of protection offered by the current directive. Subsequently, Mr. Wolfsen explained that one of the key priorities of the EDPB is to support stakeholders and especially SMEs with practical guidance and examples, specifically referring to the recently adopted guidance regarding Data Breach Notification[3], the storage of credit card data for the sole purpose of facilitating further online transactions[4], the final version of the much awaited recommendations on supplementary measures for international transfers[5], that was adopted on the next day, and the forthcoming guidance on pseudonymization and anonymization. Finally, he stated that the EDPB is developing a new tool for SMEs in order to bring together and under one single platform all the available practical guidance developed by national DPAs. Answering a question, Mr Wolfsen stated that the topic of dark patterns is under discussion in several of the EDPB's subgroups.

2.3 INVITED TALKS

Elise Lassus from the Fundamental Rights Agency presented the activities of the agency with respect to AI and fundamental rights. These activities date back from 2017 and include papers on discrimination, on preventing unlawful profiling, on data quality and AI, on facial recognition technology for LEAs and last year on AI and fundamental rights, which was presented during the conference. Current work also includes algorithmic biases. She noted that in AI, the focus on ethics might be quite attractive but when taken in isolation, they are voluntary, non-enforceable and non-standardized. Fundamental rights, on the contrary, are legally binding, hold the state accountable and examine the harms of individuals. FRA's research spanned on 5 Member States, different areas of use of AI and different levels of automation and complexity. According to the research the most important reason for using AI was increased efficiency. Mrs Lassus pointed out that efficiency alone cannot justify an interference with fundamental rights. Interviewed personnel stressed the importance of human intervention, but without being able to accurately describe how this intervention happened. They also feel uncertain on how data protection legislation is applied. The study showed that there's lack of in-depth analysis of non-discrimination issues, e.g. on the rights of the child or on people with disabilities, although interviewed persons believe that their system does not lead to discrimination. Another conclusion was that in order to ensure access to an effective remedy, transparency and access to information are crucial including the need to explain the automated decision, without relying on traditional ways of providing remedies and information. The study also showed that an AI system can also impact almost all fundamental rights. FRA's recommendation is that any future AI regulation needs to be evidence-based, rights-based and applicable in practice taking into account the full scope of fundamental rights. The agency calls for targeted research to ensure non-discrimination, for more guidance on data protection and AI and for more transparency.

[2] See https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en
[3] See https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en
[4] See https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022021-legal-basis-storage-credit-card_en
[5] See https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Philippe Gerard, adviser at European Commission DG CONNECT, followed, who explained the Commission's initiative on digital principles, which is part of the Commission's vision for digital transformation by 2030 that was published on March 2021. These principles should reflect the European way for the digital society, with people at the centre of a sustainable and prosperous digital future. Users, policy makers and digital operators will use these principles and the digital citizenship for the benefit of everyone. The principles are essential concepts, based on the already existing EU values which remain unaffected, serving as a foundation for a human-centric, secure and open digital environment. The principles were put in public consultation that is open until the 2nd of September 2021[6]. One section of the proposed digital principles is dealing with the need for a secure and trusted online environment, including confidentiality of electronic communications and the protection of information stored on devices. Philippe Gerard encouraged everyone to participate to the consultation. Building on the public consultation, the Commission will make a proposal for a joint inter institutional solemn declaration with the European Parliament and the Council by the end of 2021.

2.4 PANEL SESSION I: SECURITY OF PERSONAL DATA: LESSONS LEARNT AND CONSIDERATIONS FOR THE "NEW" NORMALITY

Panellists: Petros Efstathopoulos (NortonLifeLock), Lilian Mitrou (University of the Aegean), Piotr Drobek (Polish DPA), Moderator: Prokopios Drogkaris (ENISA)

Prokopios Drogkaris, after introducing the panellists, introduced the topic of the session, by noticing that several of the keynote speakers have already touched upon the impact of the pandemic and new legislative proposals like the new AI regulation proposal on data protection and on the security of personal data.

Petros Efstathopoulos started his talk referring to the recent Norton Labs Consumer Cyber Safety Pulse Report[7]. Current threats are following covid-19, so the primary activity they notice are pandemic related scams. Phishing campaigns are still the No. 1 threat to Cyber Safety globally and these included vaccine-oriented scams, tax refund and financial relief scams as well as tech support scams. For the near future, they expect a shift to post covid-19 scams, like vaccine passport fraud, ransomware attacks and supply-chain attacks. Mr. Efstathopoulos noted the fast rising of stalkerware, a form of malware designed to secretly monitor a person's electronic activity, which is a particular danger for sensitive social groups, like victims of domestic abuse. He then elaborated on five specific examples of threats for consumers: Cryptocurrency, Phishing and smishing, Tax fraud, Covid-19 vaccination scams and Gaming threats.

Lilian Mitrou focused on the lessons learnt from the pandemic in terms of privacy and data protection, since technology was used in the fight against covid-19 with several engineering solutions, like the covid-19 tracing apps. Technology was used also as the answer to the challenges induced by lockdowns ad forced physical distave, while at the same time, introducing risks to the rights and freedoms of individuals, that were unthinkable before the pandemic. Especially, in times of crises, it is crucial for public and private actors to conduct effective and appropriate balancing exercises to ensure that public health protection measures do not disproportionally affect fundamental rights. She underlined that - as EDPB and EDPS statements also recall at any chance - data protection does not constitute an obstacle for fighting even this complex and unpredictable the current pandemic . Prof. Mitrou focused on digital covid-19 certificates. These are not associated with the pandemic, but with the motto "back to normal life" and enable the individual to safely enter places and travel. She reminded that vaccination cards were already used for people travelling to specific distant countries

[6] See https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-set-european-digital-principles
[7] See https://www.nortonlifelock.com/blogs/norton-labs/june-2021-cyber-safety-pulse-report

anddhe explained what the EU digital green certificate will contain . According to L. Mitrou the EU regulation tries to achieve a balance between objectives of general interest and the right to self-determination as well as the respect to the fundamental rights to privacy and data protection. According to Professor Mitrou, the main challenges are connected to the further use of this certificate, e.g. the storage, the potential uses and users, the retention period. Examples from Member States like Germany and Austria indicate that further use of these data is possible. But any plan for incorporating a digital certificate for everyday use, should include the use of anonymous and untraceable information unless explicitly provided by law. Identities should be securely verified and users of verification should be strongly authenticated. Security measures are needed to mitigate information security risks such as certification forgery. However, these certificates are not immune to impediments that may affect their adoption and acceptance, just as the contact tracing apps. Any solution will have to pass the test of efficiency, proportionality, social, ethical and legal acceptability. Professor Mitrou finished by stating that the main challenge for the use of these certificates is that in order to safeguard security, accuracy and integrity we would probably have to sacrifice privacy, so a trust framework that protects both values, security and privacy, is needed.

Piotr Drobek stated that the pandemic was the catalyst for the rapid transfer of various services to the cyberspace, without any prior preparation either from organizations or from individuals. In terms of covid-19 tracing apps, it is now obvious that the implementation of even the best app, is not sufficient to fight the pandemic. For the digital green certificate, it should be noted that its use should be time limited and there are guarantees such as storage prohibition. But the regulation does not cover the use of the certificate within Member States in several sectors. Thus, a major risk is the potential use of these data for other purposes and the conditions of use should be explicitly defined in national laws and proper apps should be build. According to his opinion, any initiatives in this field should be coordinated at EU level. Piotr Drobek stressed the need for more transparency and proper DPIAs.

In the Q&A section of the panel session, Lilian Mitrou reminded that the French DPA has allowed the mandatory use of the certificate for events with more than 1000 participants[8] but such decisions should be taken while considering the specific context and situation. Priority to vaccinated individuals is not a purely data protection or security issue, but is mainly ethical question related to well-being freedom and discriminationOn the one side vaccinated persons should be able to enjoy a "safe" and free environment but on the other side stigmatization risks should be faced. The data protection issue is related to how one can regulate the strict use of the certificate, without allowing storage and any unlawful further processing . Piotr Drobek added that even with covid-19 apps, the main issue was how to build trust with the users and that the digital green certificate should be time and purpose limited.

Petros Efstathopoulos explained that online tracking is different than the above covid-19 activities and solutions to prove the identity and attributes of an individual. Technology provides solutions that are respectful of user rights. Research around verifiable credentials, zero knowledge proofs, self-sovereign identities provide strong safety and cryptographic guarantees, are standardized and provide selective disclosure under the control of the individual. This technology is quite mature and can be used as long as it is supported by issuing authorities and can provide to users the option to decide what's best for them.

In her closing statement, Lilian Mitrou argued that AI has played a strong role during the pandemic, for analysis, prediction or research. But the tools that were implemented should withstand the "high risk" test of the AI regulation. The GDPR already provides the tools to deal with these uses, through DPIAs, although Prof. Mitrou stated that "especially when taken in the middle of a crisis, no decision is perfect" while mentioning that . in this period several DPIAs were conducted under emergency and without having the time and possibility for consultation

[8] See https://www.cnil.fr/fr/covid-19-la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-du-passe-sanitaire

and trust building dialogue with stakeholders. Piotr Drobek fully agreed, adding that DPIAs are dealt as a formal obligation. He argued that in addition to the risk based approach, the precautionary principle should be taken into account, especially in relation to the effects of the AI system to individuals. The GDPR's article 22 provides a guarantee which might not always be effective. Petros Efstathopoulos stated that since AI is as good as the data you feed it, the challenge is where to draw the line between utility and privacy. Finding the right balance will benefit AI research while preserving individual rights.

3. DAY 2 – JUNE 18, 2021

3.1 OPENING REMARKS

Juhan Lepassaar, Executive Director of ENISA, welcomed everyone from all over the world to the conference and explained that the approaches of security by design and privacy by design bring together the respective communities. Cybersecurity and privacy are different sides of the same coin and are closely interlinked, as the pandemic demonstrated. The role of the APF is to bring together these two sides and investigate how these symbiotic areas can strengthen in practice. Two examples are the e-Privacy Regulation, since proper protection of metadata is vital for cyber resilience, and the new concept of European ID that has been proposed.

3.2 KEYNOTE TALK

Lorena Boix Alonso (Director for Digital Society, Trust and Cybersecurity in DG CONNECT of the European Commission) explained that the term "Digital" is the focus of the Commission, but not in any way, but at the service of citizens. That's why their privacy is so important. New legislation is designed with privacy by design in mind. The e-Privacy Regulation which is currently in trilogue, will also foster innovation, updating the provisions to recent technological advancements. The Digital Green Certificate is another example of how the legislation respects data protection and individual rights, since it is designed with privacy at the centre. This certificate had to comply with three functional principles. It had to be easy to use, it had to be secure and it had to respect privacy by design. She also elaborated on the technical characteristics of the certificate that successfully implement these principles, also stating that several third countries are willing to use a similar solution. Lorena Boix Alonso continued by explaining the new proposal for a European e-ID, to be used across borders. What is proposed will provide the citizen with full control over his or hers data, so that one can be able to demonstrate only the type of information needed. It will be provided in the form of a secure digital wallet and Member States will store data and the type of information. During the pandemic, Member States have observed a vast increase in the use of e-ID solutions that do not always provide proper privacy controls. Nowadays, citizens demand the cross-border use of e-IDs, and as several Eurobarometers have clearly shown, with respect to data protection. Providers of the wallet will not be able to collect any data from it and they should not be able to combine these data, unless for the functioning of the wallet. Trust service providers can provide certain types of information (e.g. professional qualifications) in a fully functionally separated way. In closing, she stated that these examples show how technology can help privacy and also how the EU makes sure that privacy is foreseen in every piece of new legislation. In that way, we are not going against innovation, but we are pushing markets. And clearly, it's not always about legislation. EU is funding research in these areas and several interesting projects are currently in development, like the BPR4GDPR[9] and the DEFeND[10] projects.

3.3 PANEL SESSION II: EPRIVACY REGULATION

Panellists: Birgit Sippel (MEP), Antonio Muñoz (Telefónica), Ursula Pachl (BEUC), Moderator: Kai Rannenberg (Goethe University Frankfurt)

Kai Rannenberg introduced the panellists and the topic that had been selected due to the recent developments with regard to the ePrivacy Regulation. He also presented the planned schedule of this panel's discussions aiming for interaction both among the panellists and the audience.

Brigit Sippel, a MEP who is also the Rapporteur of the act in the European Parliament, initially explained the need for an ePrivacy Regulation. Firstly, the previous directive had originally been written with the idea of only binding Telcos and not other communication services (following the entry into force of the Electronic Communications Code[11], OTTs are also currently covered by the Directive), and secondly, the directive is implemented in different ways across Member States, leading to inconsistency. She also stressed that the primary goal of the Regulation should be to better protect privacy and confidentiality and not to enable new businesses. The new rules should not undermine the current level of protection, awarded under the GDPR and the current ePrivacy directive. In fact, with all the new digitization initiatives, we have to increase the level of protection for privacy in communications, also due to the Charter of Fundamental Rights. Since communication data are very sensitive, further processing for other purposes should not be permitted. Tracking should not be permitted without consent, as it is not transparent and expected and it is not happening in the analogue world, either. Most citizens cannot know if they are tracked, so the principle design should be that you are not tracked, unless you decide to be. Statistical counting can happen, but this should not lead to individual profiles. Data retention could only be done in in accordance with the limitations introduced by the courts and on the basis of a separate law. Brigit Sippel stressed the role of independent authorities to enforce the legislation and stated that it would be important that the supervision is done by Data Protection Authorities without dividing supervision into many different organizations.

Antonio Muñoz from Telefonica, representing ETNO, the European Telecommunications Network Operators' Association, highlighted that ePrivacy is not a sectorial regulation, but has great impact on Telcos. So, we need to find the right balance between innovation, competitiveness, sovereignty and privacy. Rules should also be consistent since data are used for many purposes and differences in legislation hinder innovation. Data are also the source for AI. According to his experience, the GDPR's risk based model has served to provide answers to the difficult situations of the pandemic. The introduction of use-cases within the text of the regulation will prove to be problematic, as new unforeseen technologies are arising. Rigid regulation does not always mean better protection, while flexible regulation fosters innovation and leads to European Digital Sovereignty and better protection. As an example, he indicated the use of foreign solutions for children's education during the pandemic.

Ursula Pachl presented the perspective of consumers on the ePrivacy Regulation stating that the pandemic changed the role of electronic communication services to the point that we are not only relying on them, but we depend on them. That makes even more important the need of a regulation for the companies that know so much about us, and that also includes our children. Consumers have no idea about which company is tracking them and very often they have no choice to say 'no'. The regulation has already been delayed too long in the council. She argued on three key provisions. First, use of the associated metadata should be limited. BEUC is not happy with the current Council wording of art. 6 that includes undefined broad purposes.

[9] See https://www.bpr4gdpr.eu/
[10] See https://www.defendproject.eu/
[11] See http://data.europa.eu/eli/dir/2018/1972/oj

Second, in the protection of terminal equipment in art. 8, the consent of the consumer should be the corner stone and tracking walls should not be allowed. Third, in art. 10 on protection by default, she explained that it is very important that privacy protection comes embedded with the device. Concluding, she stated that the need for these rules is extremely important, that we do need to strike a balance with the commercial interests but the fundamental rights and the freedoms, privacy and autonomy of persons are important for our entire society.

Brigit Sippel presented some of the discussion items of the trilogue for articles 10, 8 and 6 and argued that the privacy principles should be respected and should be implemented in the text. Antonio Muñoz explained that a flexible regulation does not mean freedom for any use of data but using data to develop new technologies that could serve people. So, further compatible processing can be done with the guarantees of art. 6.4 of the GDPR and not for earning money. Availability of technology, as shown in the pandemic, is in favour of people and the balance of the regulation should be between technology, privacy and innovation and not commercial interest vs privacy. Ursula Pachl replied that trust should be deserved and currently consumers show that they are not interested in personalization, unless they are able to decide on that proactively. So, leaving the choice for the compatibility of further processing on the companies worries them, especially as the GDPR experience is not that positive in terms of the proactivity of the supervisory authorities.

In the Q&A section of the panel several participants contributed questions and comments, to which the panellists reacted. Brigit Sippel stated that cookies and ‘consent fatigue’ is an issue, but the goal of the Regulation is a Privacy by Default approach. Technology can provide solutions that respect this principle and allow any user to change the privacy setting according to his/hers wishes. However, the task of the legislators is to tackle issues of misuse and disrespect of users and we need binding rules to achieve that and not to deal with conflicts after they happen, since authorities take time to resolve cases, especially with the big players. Antonio Muñoz stated that privacy is a competition factor. Telcos have done great efforts to respect privacy legislation and not only because it is a fundamental right, but also because of its competitive market value. Their goal is to use data in order to understand patterns of society, pseudonymised data with minimal impact to individuals. He added that tools already present in the GDPR, like certifications and seals, auditing tools and BCRs, could play a role in the ePrivacy Regulation to increase people’s trust in Telcos. Ursula Pachl explained that the use of intrusive cookie banners and dark patterns is not compliant with the GDPR and the ePrivacy directive. However we are faced with several intrusive notices because the surveillance model is already in place and that is a situation that should change. She noted that the level of consu;er complaints on the Telco industry is high for several years, although not in privacy issues, but that indicates that it’s not the industry sector that consumers can easily trust. In reply to Antonio’s remark on the further use of information, she stated that it should be up to the user to decide, and if users trust the companies, they will easily consent to such a use of their data. She also mentioned that users should be asked only once, and that dark patterns are an increasing problem, since consumers are manipulated to consent. That issue of dark patterns can also be tackled through consumer protection legislation or the Digital Services Act. Brigit Sippel added that even the use of pseudonymous data for research purposes cannot be considered as without effects to individuals, reminding of the case of Cambridge Analytica. For certificates as means to get back trust she explained that it is not the answer to the problem, for several reasons, e.g. because of the large number of available certifications or the rapid change of technology that might make past certifications obsolete. On the other hand, transparency and cooperation with DPAs could provide a safer solution.

Juhan Lepassaar was invited to intervene towards the end of the session and emphasised that the regulation is needed as soon as possible. It is not only a matter of privacy but it also affects security and the resilience of the systems that we build in the digital society. This urgency has been highlighted by the pandemic where a number a services became mainstream, leading to immense data sharing. That’s why stronger rules are needed to adequately protect these data.

In the final round of statements, Ursula Pachl stressed the urgency of the ePrivacy regulation, calling the negotiators to do their best efforts and that, at the very least, decision makers should ensure the same level of protection as the current legislation. She also called on citizens to apply pressure to their government and MEPs and empower civil society organizations that represent consumer's interests. Antonio Muñoz argued that the current legislation that dates from 2002, cannot tackle new technological challenges, but it is important to have the smartest rules as possible. People should trust players that try to be more transparent through transparency centres and try to be in touch with their customers. A smart customer should have a smart provider and smart authorities. Brigit Sippel agreed on the urgency of the legislation but stated that she can't provide a date, especially taking into account the time it took the European Council to decide on a common position. She argued that it is time to find a better way to deal with new technologies, protecting privacy, and it would be great if companies and researchers could develop a way to comply with available standards and legislation, so it should be a common effort from different areas and sectors to ensure that privacy will still exist in the next century.

3.4 INVITED TALK - OUT OF CONTROL: HOW CONSUMERS ARE EXPLOITED BY THE ONLINE ADVERTISING INDUSTRY

Final text pending approval by the speaker

3.5 PANEL SESSION III: TOWARDS ENGINEERING DATA PROTECTION PRINCIPLES

Panelists: Veronica Jarnskjold Buer (Norwegian DPA), Massimo Attoresi (EDPS), Monika Adamczyk (ENISA), Moderator: Peter Kraus (EDPB)

Peter Kraus introduced the panellists and presented the panel's topic which was connected with the concepts of data protection by design and by default. The EDPB has provided guidance on this topic[12] in order to operationalize these concepts and all the panellists had been involved in the drafting of this text.

Monika Adamczyk, from ENISA, focused on pseudonymization, one of the measures proposed by the GDPR. It is a measure appropriate not only for data minimization but also for security. ENISA has already published relevant recommendations[13]. She briefly mentioned several pseudonymization techniques, like simply replacing id's with numbers, using masking, obscuring data, using hashes, symmetric or asymmetric encryption. Choosing the right technique is not trivial task. A data controller should take into account several factors, the purpose of the processing, use of data after pseudonymization, the actors and apply a risk based approach. ENISA in the aforementioned recommendations proposes three approaches for pseudonymization policy.

Massimo Attoresi, deputy head of technology and privacy unit of the EDPS, presented the agency's activities for data protection by design and by default. The IPEN initiative was launched on 2013 to fill the gap and bring dialogue between lawyers and engineers. After the GDPR took effect, when these concepts became mandatory obligations, the IPEN is trying to investigate the state of the art on these two areas. In previous years the role of encryption was analysed, whereas the pandemic led to a global privacy engineering exercise on covid-19

[12] See https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
[13] See https://www.enisa.europa.eu/news/enisa-news/cybersecurity-to-the-rescue-pseudonymisation-for-personal-data-protection for available reports

tracing apps. The effectiveness of the protection of individuals depends on a multidisciplinary analysis of the problem in its entirety. This year, with the emergence of the AI regulation, IPEN focused on the use of synthetic data instead of real data, as one of the possible technologies to mitigate privacy risks, in certain use cases, e.g. in machine learning models, or software testing. Massimo Attoresi stated that privacy engineering needs a community of practitioners and that its success will depend on how much it will be integrated in the existing technological practice, just as security is nowadays integrated in ICT. He also presented several initiatives of the EDPS like providing guidance and inspection tools and collaborate with other DPAs. He finished by declaring that data protection by design and by default is always in the centre of the EDPS's opinions.

Veronica Jarnskjold Buer, the head of the technology department of the Norwegian DPA, noted that the Norwegian DPA has published guidance for software development with Data Protection by Design and by Default[14]. At the same time, they launched a relevant annual competition for professionals and students, in order to increase awareness and demonstrate good practical examples. Although none of the winners perfectly complied with the whole of the GDPR, they have managed to successfully incorporate at least one of the key elements of the regulation. She proceeded by presenting the winners of the four previous years. Solutions that won exhibited elements like supporting the access of user rights, online access -without downloading- to rich but anonymized data for research purposes, a method for creating synthetic test data without losing the existing business logic, anonymous tokens which deliver one-time unlinkable signatures and allow for authentication and anonymity after the first identification phase.

Answering a question Monika Adamczyk stated that measuring the improvement of data protection, after data protection by design techniques have been implemented, would be difficult. One of the ways would be through regular risk assessment that would identify whether risks are still important. It is also important to assess how well the data are used in respect of the purpose of the processing. Massimo Attoresi added that the continuous assessment is important even for encryption, reminding the evolution of quantum computing. Veronica Jarnskjold Buer pointed out that to make digital society more privacy friendly, developers should be trained so they understand the essence of privacy by design, so they can code the requirements in their products. Massimo Attoresi suggested a template of a project chart, with steps to implement functional and non-functional requirements. Monika Adamczyk mentioned that it is also crucial that the data protection by design is part of the organization's culture. Often, although there are good intentions, functionality and delivery of product prevail. All panellists agreed on the need to use a privacy framework and relevant DPAs guidance (e.g. the Norwegian on software development and guidance on DPIAs from EDPB and several DPAs) when developing new products.

In the final round of statements Massimo Attoresi explained that the EDPS that has an important role as advisor to the legislator is thinking to provide in the future more hands on support to institutions. Monika Adamczyk added that ENISA is continuing work in Privacy Enhancing Technologies preparing new recommendations on advanced techniques, like homomorphic encryption, zero knowledge proof, secure multi party computation and is watching the rapid advancements in order to provide practical advice. Veronica Jarnskjold Buer stated that they will continue their activities. In the strategy of the country's DPA for the next two years, is to focus on the notions of data protection by design and by default. She also reminded the establishment of a sandbox in the DPA, and stated that it is expected that future projects will be more technology oriented.

[14] See https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/

3.6 CLOSING REMARKS

Monika Adamczyk thanked the participants, briefly summarized the second day of the conference and presented the location for the 2022 Annual Privacy Forum, which is going to take place in Warsaw on June 23 and 24, 2022. The co-organizers will be the universities Cardinal Stefan Wyszynski University and Kozminski University. Piotr Drobek and Professor Przemyslaw Polanski represented the two institutions and invited everyone in Warsaw, by using a short video introduction. Ms. Adamczyk closed the 2021 edition of the event, expressing the hope that next year's event will be organised as a physical event.