Dear Reader,

I am Camilla Ravazzolo and as the new EFAMRO's Head of Policy and Standards, I will be publishing your Monitoring Report. I am committed to delivering the most useful instrument of information updates. This is why I am currently conducting interviews to gather member's inputs, comments and suggestions on the Reports' schedule, content and format. If you are interested in letting me know your opinion on any of these aspects, please don't hesitate to reach out.

Looking forward to engaging with each and every one of you,

Kind regards,

Camilla Ravazzolo

Camilla.ravazzolo@efamro.eu

Monitoring Report – 28/06/2019 (No. 16 of 2019)

The EFAMRO monitoring report covers selected legal and regulatory developments and events in data protection of particular interest to the European research sector.

Table of Contents

Data protection

Digital Single Market: Commission publishes guidance on free flow of non-personal data

The European Commission published a new guidance on the interaction of free flow of non-personal data with the EU data protection rules.

The Regulation on the free flow of non-personal data, applicable as of 28 May 2019, aims at removing obstacles to the free movement of non-personal data across Member States and IT systems in Europe. The Regulation ensures:

- Free movement of non-personal data across borders: every organisation should be able to store and process data anywhere in the European Union
- The availability of data for regulatory control: public authorities will retain access to data, also when it is located in another Member State or when it is stored or processed in the cloud
- Easier switching of cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can port data between cloud service providers and back into their own IT environments.

The focus of the guidance is the interaction between the free flow of non-personal data regulation and the GDPR. It particularly addresses:

- The concepts of personal and non-personal data, and their combination in so-called 'mixed datasets'.
- The principles of free movement of data and the prohibition of data localisation requirements
- Data portability.

The guidance also covers self-regulatory requirements set out in the two Regulations.

The process of real-time bidding (RTB) used in online programmatic advertising is at odds with data protection law, the UK Information Commissioner's Office (ICO) has ruled.

The regulator has been investigating how personal data is used when online ads are bought and placed on websites, specifically whether the process complies with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

Under data protection law, people must give their explicit consent to have their data used to serve them with ads, but the ICO ruled that this is not currently happening.

Simon McDougall, executive director for technology and innovation at the ICO, said: "Sharing people's data with potentially hundreds of companies, without properly assessing and addressing the risk of these counterparties, raises questions around the security and retention of this data."

Current practices for processing personal data – particularly the processing of special category data without explicit consent – are 'problematic', the ICO said.

It also expressed concerns about the complexity of the data supply chain, saying that relying on contractual agreements to protect data is not enough.

The ICO has warned that it expects the industry to change its approach to privacy notices, use of personal data, and the lawful bases applied within RTB.

McDougall said: "We want to see change in how things are done. If you operate in the adtech space, it's time to look at what you're doing now, and to assess how you use personal data. We already have existing, comprehensive guidance in this area, which applies to RTB and adtech in the same way it does to other types of processing – particularly in respect of consent, data protection by design and data protection impact assessments (DPIAs)."

The ICO will work with the industry over the next six months and may conduct another review later in the year if its demands are not met.

Research Live article here

European Court of Justice hearings to determine future of Privacy Shield, SCCs

The EU-U.S. data-sharing arrangement faces its biggest obstacle yet, as the Court of Justice of the European Union is looking at two cases challenging its legality in the coming weeks.

Privacy Shield has been under fire ever since it was negotiated by the European Commission and U.S. Department of Commerce as a replacement for the faulty Safe Harbor agreement. The contention is that U.S. surveillance agencies have too much unfettered access to Europeans' data.

It will come as no surprise to privacy professionals that the man behind one of those cases is Max Schrems, the Austrian whose case brought down Safe Harbor in 2015.

The new case is fundamentally the same and should worry companies relying on Privacy Shield or standard contractual clauses to use Europeans' data. As with the Safe Harbor case, the contention is that U.S. surveillance agencies have too much unfettered access to Europeans' data.

The original complaint was made more than five years ago and is based on Edward Snowden's disclosures that Facebook allows U.S. agencies access to personal data under schemes such as "PRISM." The European Court of Justice took these revelations at face value when ruling Safe Harbor illegal.

Following hearings before the Irish High Court in 2017, Irish judges found that the U.S. authorities did indeed engage in mass processing of Europeans' data and referred 11 questions relating to whether standard contractual clauses provide an adequate level of protection.

IAPP has the story here

Aggregating over anonymized data

Folks who want to make data-driven decisions naturally want data to make those decisions. They want to slice and dice that data to learn every useful trend. Sometimes, that data is public or otherwise not in need of anonymization. However, in many cases, the data needs to be anonymized, transformed so that the original user can be in no way identified, and this is where things turn complicated.

This is the fourth in a series of Privacy Tech posts focused on privacy engineering and UX design from Humu Chief Privacy Officer Lea Kissner.

EDPS: Internet Privacy Engineering Network discusses state of the art technology for privacy and data protection

The 2019 Internet Privacy Engineering Network (IPEN) workshop took place on 12 June in Rome, Italy. This year's workshop focused on state of the art technology in data protection by design, in an effort to help establish a common understanding of this concept.

Under the EU's General Data Protection Regulation (GDPRit is now a legal obligation to consider personal data protection from the early project stages when designing technological solutions. This includes embedding measures into new technologies to ensure that the fundamental rights of individuals are adequately protected when their personal data is processed. Controllers and developers, regulators and legal experts all need to understand what they should – and should not – consider as state of the art technology to be able to design and implement measures to effectively protect individuals.

The workshop explored four key areas: the concept of state of the art in relevant fields, the consideration of business models enabling individuals to be in control of their data, privacy engineering, pseudonymisation and anonymisation. Presentations and recordings from the workshop will soon be available on the EDPS website. After another successful session, the EDPS looks forward to engaging with IPEN in future events to ensure a stronger, collaborative and effective approach to privacy engineering.

IPEN Rome Workshop 2019
EDPS Press Release

EDPS: Defending individual rights: a focused approach to data processing

The risk-based approach is one of the requirements put into focus by both the General Data Protection Regulation (GDPR) and the equivalent rules for EU institutions (GDPR for EUI). This approach requires data controllers and processors to take into account the risks of each data processing operation they carry out – specifically the risks to individuals and their fundamental rights. Data protection impact assessments and personal data breach notifications are two examples of situations where a specific risk assessment is now required.

As well as identifying the risks associated with a data processing operation, controllers need to show that they have a risk management strategy in place to address the risks to individual rights that are identified. In this way, they ensure accountability, through being able to demonstrate their compliance with data protection rules. This risk mind-set strengthens protection for the individuals whose data is being processed by increasing the responsibility taken by the controller.

The risks posed to individual rights can depend on a range of factors: the processing operations, the controllers themselves, the safeguards in place, and more. Different organisations face different risks and need to assess and then mitigate those risks to people and their rights on an individual basis.

Risk management for personal data requires more than just expertise in information and IT security – these very human challenges require a human-centric response. Data Protection Officers (DPOs) play an essential role in ensuring that controllers are informed and aware of any relevant risk to individuals. DPOs should therefore support information and IT security experts in the development of effective risk management processes.

It is almost impossible to eliminate risk from personal data processing. Data controllers and processors therefore need to be able to assess and demonstrate examples of what constitutes acceptable risk. Technical security solutions alone cannot solve the challenge of information security and data protection. Managers must support the development and implementation of policies, and ensure there are resources available to counter any risks to individuals in their data processing activities.

There is a clear and simple message here: before beginning any data processing activity, make sure you are aware of the risks it poses to the individuals concerned – by adopting a risk mind-set!

Artificial Intelligence and ethics

UK government releases "A guide to using artificial intelligence in the public sector"

The guidance covers how: to assess if using AI will help you meet user needs, the public sector can best use AI, to implement AI ethically, fairly and safely.

The Alan Touring Institute published Understanding Artificial Intelligence Ethics and Safety: the most comprehensive guidance on the topic of AI ethics and safety in the public sector to date. It identifies the potential harms caused by AI systems and proposes concrete, operationalizable measures to counteract them. The guide stresses that public sector organisations can anticipate and prevent these potential harms by stewarding a culture of responsible innovation and by putting in place governance processes that support the design and implementation of ethical, fair, and safe AI systems.

Guidance available here

Understanding Artificial Intelligence Ethics and Safety available here

Oxford University to Use Teradata For Marketing Research

US & UK – Oxford University's Saïd Business School is partnering with data intelligence firm Teradata to use its data analytics platform as part of the Oxford Future of Marketing Initiative.

As part of the partnership, San Diego-headquartered Teradata will also fund a postdoctoral research fellowship on the Future of Marketing research team.

The academic and industry initiative conducts research on the challenges and opportunities for marketing in future. Facebook, L'Oréal, Allianz Insurance and Kantar are among the other industry partners.

Teradata's Vantage integrates descriptive, prescriptive analytics, machine learning and visualisation tools within one platform.

Andrew Stephen, associate dean of research and L'Oréal professor of marketing at Saïd Business School, said: "Given that a large part of the future of marketing involves advanced data analytics and machine learning at scale, working with Teradata and having access to Vantage will allow our researchers to develop new capabilities and answer new research questions around the applications of machine learning to real-world marketing problems."

Martyn Etherington, chief marketing officer at Teradata, added: "This partnership allows both of our organisations to continuously create and share ideas, research insights, and customer experiences."

Research Live has the story

From Europe

Italy: Garante approves code of conduct on processing for commercial information purposes

The Italian data protection authority ('Garante') announced, on 21 June 2019, that it had approved a code of conduct on the processing of personal data for commercial information purposes ('the Code of Conduct'), under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). In particular, the Code of Conduct identifies the adequate guarantees and methods that data controllers and processors in the commercial information and credit management sector should implement when processing personal data to protect the rights of data subjects. The Code of Conduct states that adhesion to the Code of Conduct may be used as an element to demonstrate compliance with the GDPR.

You can read the Code of Conduct, only available in Italian, here.

Italy: Ministry releases reply on data recording in medical databases

The Ministry of Labour and Social Policies ('the Ministry') published, on 28 May 2019, Reply No. 4/2019 ('the Reply') on the use of automated means to record patients' data on business' databases, following a request by the National Federation of Surgeons and Dentists' Professional Associations ('the Associations'). In particular, the Ministry outlined that the use of automated means is permitted for any kind of data, as long as the employer and the competent doctor adopt joint solutions to ensure that access to those data is only granted to the competent doctor, and not to the employer and the database administrator.

You can read the Reply, only available in Italian, here.

Ireland: Five Steps to Secure Cloud-based Environments

Cloud-based environments offer many advantages to organisations; however, they also introduce a number of technical security risks which organisations should be aware of, including data breaches, hijacking of accounts, and unauthorised access to personal data. Organisations should determine and implement a documented policy and apply the appropriate technical security and organisational measures to secure any cloud-based environments they utilise. The DPC has prepared guidance to assist organisations understand their obligations with regard to the security of personal data, and to mitigate their risks when utilising a cloud-based environment.

Five Steps to Secure Cloud-based Environments - Full Guidance Note

Netherlands: AP issues recommendations on DPOs in hospitals

The Dutch data protection authority ('AP') issued, on 24 June 2019, recommendations ('the Recommendations') for data protection officers ('DPOs') and boards of directors, concerning DPOs operating in hospitals, following an investigation. In particular, the AP highlighted that DPOs operate well in the 11 investigated hospitals and that mainly smaller hospitals could still improve by introducing more written guarantees. Furthermore, the AP noted that the Recommendations can be applied to the entire industry.

In addition, the Recommendations suggest that DPOs keep a good balance between his/her advisory and supervisory role, provide more attention to supervision, prevent conflicts between the two roles, and make clear internal agreements in relation to the division of responsibilities. Furthermore, boards of directors are recommended to, among other things, implement internal guidelines in a privacy policy on the DPO's position and ensure that the DPO receives sufficient resources.

You can read the press release here and the recommendations here, both only available in Dutch.

Poland files complaint with EU's top court over copyright rule change

Poland has submitted a complaint to the European Union's top court against copyright rules adopted by the bloc in April to protect Europe's creative industries, which Warsaw says may result in preventive censorship.

Google will have to pay publishers for news snippets and Facebook filter out protected content under copyright rules aimed at ensuring fair compensation for the EU's $1 trillion creative industries.

Poland has said the overhaul was a step backwards, arguing that the filter requirement could lay the foundation for censorship.

Reuters has the story.

UK: SCC publishes secure by default self-certification form and guidance

The Surveillance Camera Commissioner ('SCC') published, on 20 June 2019, a secure by default self-certification form and guidance for manufacturers of video surveillance systems on secure by default and secure by design requirements ('the Guidance'). In particular, the SCC highlighted that the self-certification form allows manufacturers of surveillance camera devices to clearly demonstrate to the SCC that their products meet minimum security requirements to be awarded the 'secure by default' branding. In addition, the Guidance outlines several elements such as default passwords, encryption and remote access that require mandatory action by the manufacturer to ensure products meet security requirements.

You can read the press release here and the guidance here, and download the form here.

From the world

Canada: Bill C-76 Canada Elections Act

Bill C-76 came into effect on June 13, 2019 and election surveys conducted during the pre-election period and the election period are now classified as regulated activities by Elections Canada.
The Canadian Marketing Research and Intelligence Association (MRIA) has made us aware that it does not matter who commissioned the survey; it is now considered a regulated activity.

Bill C-76 Canada Elections Act

Egypt: Communications Committee approves data protection bill

DataGuidance by OneTrust confirmed, on 24 June 2019, with Dr. Mohamed ElFar, Counsel at Helmy, Hamza & Partners, member firm of Baker McKenzie International, that the Communications Committee within the Egyptian House of Representatives had approved the data protection bill ('the Bill') on 17 June 2019.

ElFar highlighted, "[the Bill] should be moved to the General Assembly to be discussed and approved before being sent to the President to issue it as a law".

More information to follow

South Korea: KCC announces adoption of ICNA amendments regarding children's location information

The Korea Communications Commission ('KCC') announced, on 24 June 2019, its adoption of amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection 2001 ('ICNA') in order to strengthen the protection of children's location information, and released an explanation ('the Explanation') on the same. The Explanation specifies processes for obtaining children's legal representatives' consent through email, phone calls, or websites, among other methods. In particular, the Explanation notes that additional confirmation will be required if this consent is obtained through a website, such as through a text message or by assessing the validity of credit or debit card details.

The KCC stated that it intends to continue the current system until the end of this year in order to minimise disruption.

USA Illinois: Assembly passes bill amending genetic information act

The Illinois General Assembly ('the Assembly') passed, on 21 May 2019, House Bill 2189 ('the Bill') which seeks to amend the Genetic Information Privacy Act. In particular, the Bill amends the definition of 'genetic testing' to also include 'direct-to-consumer' commercial genetic testing and also seeks to prohibit a company which provides 'direct-to-consumer' commercial genetic testing from sharing any genetic test information or other personally identifiable information about a consumer with any health or life insurance company without the consumer's written consent.

You can read the Bill here and track its history here.

Upcoming Events

October 2019

European Big Data Value Forum 2019

14th - 16th October, Helsinki Finland

The European Big Data Value Forum (EBDVF) is the main event of the European Big Data and Data-Driven Artificial Intelligence (AI) Research and Innovation community.

The European Big Data Value Forum 2019 aims to continue the success of previous editions, where on average every year around 700 industry professionals, business developers, researchers, and policymakers coming from 40 different countries attended the event.

The organising committee of this event includes, in addition to BDVA , the EC and VTT , multiple Finnish industrial, Innovation and Research players as well as international companies and other research institutions.

Read more: More information