Monitoring Report – 15/03/2019 (No. 7 of 2019)

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

The EDPB recently concluded its eighth plenary session. Statements issued on the interplay of the ePrivacy Directive and the GDPR highlighted the EDPB view that national data protection authorities are competent to enforce GDPR rules even though ePrivacy rules apply and will assess breaches of both as separate infringements. EDPB has also called upon EU legislators to intensify efforts towards the adoption of the ePrivacy Regulation. The EDPB also adopted two opinions on the Data Protection Impact Assessment (DPIA) lists submitted to the Board by Spain and Iceland.

Bulgaria's GDPR implementing law entered into force on 2 March 2019. The Law on Amending and Supplementing the Law on Personal Data Protection (LASLPDP) modernises the original Data Protection Act from 2002. It also transposes the EU Law Enforcement Directive.

On the enforcement front continued focus on the big tech organisations. The Swedish consumer group filed comments in the ongoing investigation by the Swedish authority against Google underlining its position that Google uses deceptive design tricks to push users into location tracking and that is lacks a legal basis for processing the user's data.

The European Parliament adopted the Cyber Security Act, initially proposed by the Commission in September 2017. The Act will improve the European response to the increasing number of cyber threats by strengthening the role of the European Agency for Network and Information Security (ENISA) and establishing a common European cybersecurity certification framework for IT services, systems and equipment.

A market research ISO standard (ISO 20252) has been newly updated to maintain quality in market, opinion and social research incorporating and supplanting ISO 26362:2009 – Access panels in market, opinion and social research – Vocabulary and service requirements. It also incorporates the requirements of ISO 19731:2017 Digital analytics and web analyses for purposes of market, opinion and social research – Vocabulary and service requirements which will continue to remain available as a separate standard.

Regulatory enforcement

GDPR Complaint – Swedish consumer organisation comments on enforcement action

Sveriges Konsumenter, BEUC's Swedish member organisation, has filed comments to a response of Google in an ongoing investigation of the Swedish data protection authority. In its comments, the Swedish consumer group underlines its position that Google uses deceptive design tricks to push users into location tracking and that is lacks a legal basis for processing the user's data. [1]

Last year, together with six other consumer organisations from across Europe, Sveriges Konsumenter brought a complaint to its data protection body against Google for the company's deceptive practices to track users' location in violation of the General Data Protection Regulation (GDPR). A report published by Norwegian consumer group Forbrukerrådet triggered the complaints. The report shows that Google does not give consumers a real choice to agree or not to providing their location data, which is then used by the company for a wide range of purposes including targeted advertising.

The places consumers go to can reveal a lot about their private life. For example, religious views (e.g. if you went to a place of worship), political stance (e.g. if you attended a protest or a political party's summit), and health-related issues (e.g. if you visited a cancer treatment centre).

Norwegian consumer group Forbrukerrådet joined Sveriges Konsumenter in its reply to the Swedish data protection authority.

Regulatory guidance

EDPB – Report on 8th plenary session of the European Data Protection Board

On March 12th and 13th, the EEA Data Protection Authorities and the European Data Protection Supervisor, assembled in the European Data Protection Board, met for their eighth plenary session. During the plenary a wide range of topics were discussed.

Interplay ePrivacy Directive and GDPR

The EDPB adopted its opinion on the interplay between the ePrivacy Directive and the General Data Protection Regulation. The opinion seeks to provide an answer to the question whether the fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limits the competences, tasks and powers of data protection authorities under the GDPR. The EDPB opines that data protection authorities are competent to enforce the GDPR. The mere fact

that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.

An infringement of the GDPR may at the same time constitute an infringement of national ePrivacy rules. SAs may take this into consideration when applying the GDPR (e.g. when assessing compliance with the lawfulness or fairness principles).

Statement on the future ePrivacy Regulation

The EDPB adopted a statement calling upon EU legislators to intensify efforts towards the adoption of the ePrivacy Regulation, which is essential to complete the EU's framework for data protection and the confidentiality of electronic communications.

The future ePrivacy Regulation should under no circumstance lower the level of protection offered by the current ePrivacy Directive and should complement the GDPR by providing additional strong guarantees for all types of electronic communications.

DPIA Lists

The EDPB adopted two opinions on the Data Protection Impact Assessment (DPIA) lists submitted to the Board by Spain and Iceland. These lists form an important tool for the consistent application of the GDPR across the EEA. DPIA is a process to help identify and mitigate data protection risks that could affect the rights and freedoms of individuals. While in general the data controller needs to assess if a DPIA is required before engaging in the processing activity, national supervisory authorities shall establish and make a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. These two opinions follow the 28 opinions adopted during previous plenary meetings, and will further contribute to establishing common criteria for DPIA lists across the EEA.

Statement on the use of personal data in the course of political campaigns

In light of the upcoming European elections and other elections taking place across the EU and beyond in 2019, the EDPB has adopted a statement on the use of personal data during election campaigns. Data processing techniques for political purposes can pose serious risks, not just with regard to the rights to privacy and data protection, but also to the integrity of the democratic process. In its statement, the EDPB highlights a number of key points which need to be taken into consideration when political parties process personal data in the course of electoral activities.

During the plenary, the following Opinions were adopted:

- Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

- Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)
- Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Also, the EDPB adopted the following Statements:

- EDPB Statement 3/2019 on an ePrivacy regulation
- EDPB Statement 2/2019 on the use of personal data in the course of political campaigns

Annex I to Statement 2/2019 on the use of personal data in the course of political campaigns

Implementing legislation and other legislative initiatives

GDPR Implementation - Bulgaria

Bulgaria's GDPR implementing law entered into force on 2 March 2019. The Law on Amending and Supplementing the Law on Personal Data Protection (LASLPDP) modernises the original Data Protection Act from 2002. It also transposes the EU Law Enforcement Directive. It was adopted on 20 February 2019.

*See **LASLPDP in full** (in Bulgaria's Official Journal).*

ePrivacy Regulation – Compromise Text

Please click here to access a revised compromise proposal on the Regulation on ePrivacy.

Cybersecurity Act – Stakeholder comment

Commission Statement

The European Parliament adopted the Cyber Security Act , which European Commission President Jean-Claude **Juncker** initially proposed in his State of the Union Address in September 2017. The Act will improve the European response to the increasing number of cyber threats by strengthening the role of the European Agency for Network and Information Security (ENISA) and establishing a common European cybersecurity certification framework for IT services, systems and equipment. In

September 2018 the Commission proposed to create a European network of centres of cybersecurity expertise , which will help to reinforce research and deployment of new cybersecurity capacities in the EU. Under the next long-term EU budget, the Commission has proposed more than €2 billion to reinforce cybersecurity in the Digital Europe Programme as well as under HorizonEurope. To lay the ground work for building this network, the Commission is investing more than €63.5 million in four pilot projects . Mariya **Gabriel** , Commissioner for Digital Economy and Society, will meet tomorrow in Strasbourg a number of representatives of these projects, which involve more than 160 partners, including large companies, SMEs, universities and cybersecurity research institutes from 26 EU Member States. More information on ENISA is available online click.

European Parliament Statement

MEPs adopt the EU Cybersecurity certification scheme for products, processes and services, whilst also expressing their deep concern about Chinese IT in the EU.

On Tuesday, MEPs adopted the EU Cybersecurity Act with 586 votes to 44 and 36 abstentions. It establishes the first EU-wide cybersecurity certification scheme to ensure that certified products, processes and services sold in EU countries meet cybersecurity standards.

Parliament also adopted a resolution calling for action at EU level on the security threats linked to China's growing technological presence in the EU.

MEPs express deep concern about recent allegations that 5G equipment may have embedded backdoors that would allow Chinese manufacturers and authorities to have unauthorised access to private and personal data and telecommunications in the EU.

Chinese state security laws a threat to EU cybersecurity

They are also concerned that third-country equipment vendors might present a security risk for the EU, due to the laws of their country of origin obliging all enterprises to cooperate with the state in safeguarding a very broad definition of national security also outside their own country. In particular, the Chinese state security laws have triggered reactions in various countries, ranging from security assessments to outright bans.

MEPs call on the Commission and the member states to provide guidance on how to tackle cyber threats and vulnerabilities when procuring 5G equipment, for example by diversifying equipment from different vendors, introducing multi-phase procurement processes and establishing a strategy to reduce Europe's dependence on foreign cybersecurity technology.

They also urge the Commission to mandate the EU Cybersecurity Agency, ENISA, to work on a certification scheme ensuring that the rollout of 5G in the EU meets the highest security standards.

EU Cybersecurity Act to enable certification of connected devices

The EU Cybersecurity Act, which is already informally agreed with member states, underlines the importance of certifying critical infrastructure, including energy grids, water, energy supplies and banking systems in addition to products, processes and services. By 2023, the Commission shall assess whether any of the new voluntary schemes should be made mandatory.

The Cybersecurity Act also provides for a permanent mandate and more resources for the EU Cybersecurity Agency, ENISA.

After the vote on the Cybersecurity Act, rapporteur Angelika Niebler (EPP, DE) said: "This significant success will enable the EU to keep up with security risks in the digital world for years to come. The legislation is a cornerstone for Europe to become a global player in cyber security. Consumers, as well as the industry, need to be able to trust in IT-solutions."

Next steps

The Council now has to formally approve the Cybersecurity Act. The regulation will enter into force 20 days after it is published. The resolution on Chinese IT presence in the EU will be sent to the Commission and to member states.

Artificial Intelligence and research

High Level Expert Group on Artificial Intelligence

Please find here the draft agenda of the High-Level Expert Group on Artificial Intelligence (main group) meeting scheduled for 18-19 March. Also, please find here the slides of the AI HLEG meeting of 25 February.

Revision of ISO Market Research Standard

The market research ISO standard – ISO 20252 – has been newly updated to maintain quality in market, opinion and social research.

The revision to ISO 20252:2019 *Market, opinion and social research, including insights and data analytics –vocabulary and service requirements* aims to help researchers and research buyers support higher and more consistent quality in services including insights and data analytics.

This standard incorporates and supplants *ISO 26362:2009 – Access panels in market, opinion and social research – Vocabulary and service requirements*. It also incorporates the requirements of *ISO*

19731:2017 Digital analytics and web analyses for purposes of market, opinion and social research – Vocabulary and service requirements which will continue to remain available as a separate standard.

It will help to ensure that no matter where research is conducted, it will meet the same risk management standards of quality and constitutes a uniform benchmark for the robustness of processes and procedures when delivering research, insight and data services.

Don Ambrose, chair of the ISO technical committee that updated the standard, said: "ISO 20252 is a must-have for the research sector. Users the world over – companies, governments, research institutes, consumer associations, educational facilities, and marketing, advertising, and insights agencies – will benefit by having global compatibility, traceability and continual improvement. In addition, it will enable clients to obtain globally compatible, comparable and homogeneous feedback and make better-informed choices of service providers."

Currently, more than 315 research agencies are 3rd party certified to ISO 20252, and more than 50 research agencies are certified to the companion standard ISO 26362.

Source: Research Live

URL: https://www.research-live.com/article/news/market-research-iso-revised/id/5050612 (log-in may be required)

Upcoming Events

March 2019

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

20 March 2019, Brussels, Belgium

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

April 2019

Center for Data and Innovation: Coordinated Plan on AI

4th April, Brussels, Belgium

To remain competitive in the global race for artificial intelligence (AI), the European Union will need more investment, more workers trained in AI-relevant skills, more shared resources including data, and a regulatory environment that will foster the development and use of AI. To that end, in December the European Commission released a " Coordinated Plan on AI" which encourages all member states to develop their own national AI strategies by mid-2019 and to work with the Commission to develop common metrics to measure AI adoption.

While some member states have already created national AI strategies, others have not or have only included dimensions of AI within broader digital strategies. Moreover, every member state is different, so the policies, priorities, and financial commitments in each national AI strategy will vary.

Join the Center for Data Innovation for a discussion that will take stock of the progress achieved so far across member states; compare targets, priorities, and dimensions; and assess the extent to which these national strategies will support Europe's goal of becoming a global leader in AI.

Registration details here: https://www.eventbrite.com/e/european-ai-strategies-where-do-member-states-stand-and-where-are-they-headed-tickets-56188139237