Monitoring Report – 05/04/2019 (No. 10 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.

Final pieces falling into place with Member State implementation of the GDPR into national law. The Czech Republic adopted, on 12 March 2019, legislation that brings the GDPR's provisions into national law. The Belgian DPA has staffed up the authority appointing the first commissioner and the directors. These are the first appointments to be made to the DPA since it replaced the previous Belgian Privacy Commission in anticipation of the EU GDPR.

Protection of health-related data by public and private sectors is an important area in building public trust. The Council of Europe has issued a set of guidelines to its 47 member states urging them to ensure, in law and practice, that the processing of health-related data is done in full respect of human rights, notably the right to privacy and data protection.

The UK Department for Digital, Culture, Media and Sport (DCMS) released the 2019 Cyber Security Breaches Survey. Statistics within the report show a reduction in the percentage of businesses suffering a cyber breach or attack in the last year.

The European Parliament released a report titled "Understanding algorithmic decision-making: Opportunities and challenges." The study was created to review the potential benefits and risks when algorithmic decisions systems are used. The report covers how algorithmic decision systems can affect individuals and entities in both the public and private sectors..

Another set of ethics principles published, this time for the US based ARF (Advertising Research Foundation) adopted its first member code of conduct on ethical research and data collection.

National Implementation

Czech Republic – GDPR implementation in national law

The Czech Republic adopted, on 12 March 2019, legislation that brings the GDPR's provisions into national law. The Data Protection Act, which repeals the previous Act on Personal Data Protection, will not apply administrative fines to the public sector. The age for children to give consent for the use of online services is set at 15, law firm Wolf Theiss reports.

The new Act now needs to be signed by the President. After that, it will enter into force on the day of its publication in the Legal Gazette.

Source: Privacy Laws & Business

Belgian DPA – Appointment of Commissioner and Directors

Sidley Austin reports that on 29 March 2019, the Belgian House of Representatives appointed a new Data Protection Commissioner and four directors to the executive committee of the Belgian Data Protection Authority ('DPA').

These are the first appointments to be made to the DPA since it replaced the previous Belgian Privacy Commission in anticipation of the EU GDPR. This is therefore the first time that executive roles have been officially filled in the context of the regulator's expanded competence – including the DPA's new power to impose administrative fines of up to €20,000,000 EUR or 4 percent of an undertaking's worldwide annual revenues for certain infringements of the EU GDPR.

The executive committee sets the strategic goals, the management agenda and the annual priorities of the DPA. Companies can therefore hope to gain a greater understanding of the DPA's enforcement priorities in the months and years ahead. In particular, the regulator has stated that it will publish information about its 'vision and mission' once its strategic plan has been drawn up. Details of enforcement action against companies established or operating in Belgium may also begin to emerge in the not-too-distant future.

The new Commissioner is named as Dr. David Stevens, who previously acted as the EU Data Protection Officer of a large multinational and who has a mix of academic, in-house and private practice experience. The other appointees are as follows Director of the Knowledge Center – Alexandra Jaspar, Director of the Front Office – Charlotte Dereppe; Inspector General – Peter Van den Eynde; President of the Litigation Chamber – Hielke Hijmans. Commentators have praised the diversity of the appointees' professional backgrounds.

Since the entry into force of the EU GDPR on 25 May 2018, the previous members of the Belgian Privacy Commission have been carrying out the executive committee's roles, but on an interim basis. It is perhaps for this reason that enforcement activity and the publication of new guidance by the DPA has been more limited when compared to other Supervisory Authorities such as the UK's ICO and the French CNIL. Nevertheless the DPA confirmed in a publication dated 23 November 2018 that the lack of a newly appointed executive committee has not prevented the DPA's inspection and sanctions bodies from being fully operational, and that its first regulatory inspections have already commenced.

Source: Sidley Austin

URL: https://datamatters.sidley.com/the-belgian-data-protection-authority-appoints-first-commissioner-and-directors/#page=1

Data protection and cyber security

Council of Europe –Guidelines on health-related data

The Council of Europe has issued a set of guidelines to its 47 member states urging them to ensure, in law and practice, that the processing of health-related data is done in full respect of human rights, notably the right to privacy and data protection.

With the development of new technological tools in the health sector the volume of health-related data processed has grown exponentially showing the need for guidance for health administrations and professionals.

In a Recommendation, applicable to both the public and private sectors, the Council of Europe's Committee of Ministers, calls on governments to transmit these guidelines to health-care systems and to actors processing health-related data, in particular health-care professionals and data protection officers. The recommendation contains a set of principles to protect health-related data incorporating the novelties introduced in the updated Council of Europe data protection convention, known as "Convention 108+", opened for signature in October 2018.

Source: Council of Europe

URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=090000168093b57d

UK DCMS Releases Cyber Breaches Survey 2019 showing reduction in percentage of businesses suffering cyber breaches

UK Department for Digital, Culture, Media and Sport (DCMS) have released the 2019 Cyber Security Breaches Survey. Statistics within the report show a reduction in the percentage of businesses suffering a cyber breach or attack in the last year.

Key findings include:

- Percentage of businesses experiencing cyber breaches or attacks drops from 43% to 32%.
- New laws to strengthen data protection have had a positive impact on cyber security.
- Businesses and charities urged to train more people to help manage cyber risks.

The report suggests that reductions are partly due to the introduction of Data Protection Act and the General Data Protection Regulations (GDPR). 30% of businesses and 36% of charities have made changes to their cyber security policies and processes as a result of GDPR coming into force in May 2018.

However, those organisations that were attacked saw the median number of associated breaches rise from 4 in 2018 to 6 in 2019. The report also suggests that the average cost of a cyber-attack has risen to £4,180. These figures illustrate that threats to organisations are persistent and continue to develop in terms of sophistication and scale.

Digital Minister Margot James said:Following the introduction of new data protection laws in the UK it's encouraging to see that business and charity leaders are taking cyber security more seriously than ever before. However, with less than three in ten of those companies having trained staff to deal with cyber threats, there's still a long way to go to make sure that organisations are better protected.We know that tackling cyber threats is not always at the top of business and charities list of things to do, but with the rising costs of attacks, it's not something organisations can choose to ignore any longer.

Through the CyberFirst programme, the Government is working with industry and education to improve cyber security and get more young people interested in taking up a career in cyber. The Cyber Discovery initiative has already encouraged 46,000 14 to 18 year olds to get on a path towards the cyber security profession, over 1,800 students have attended free CyberFirst courses and nearly 12,000 girls have taken part in the CyberFirst Girls competition. The Government's initial Cyber Skills Strategy, published in December, will be followed by a full strategy later this year.

Business and charity leaders are being encouraged to download the free small business guide and free small charity guide to help make sure that they don't fall victim to cyber attacks. This is available through the National Cyber Security Centre (NCSC).

Clare Gardiner, Director of Engagement at the NCSC, said :We are committed to making the UK the safest place to live and do business online, and welcome the significant reduction in the number of

businesses experiencing cyber breaches. However, the cyber security landscape remains complex and continues to evolve, and organisations need to continue to be vigilant.

The NCSC has a range of products and services to assist businesses, charities and other organisations to protect themselves from cyber attacks, and to deal with attacks when they occur. These include the Board Toolkit providing advice to Board level leaders, and guides aimed at small businesses and small charities.Small businesses and charities are being urged to take up tailored advice from the National Cyber Security Centre. All businesses should consider adopting the Ten Steps to Cyber Security, which provides a comprehensive approach to managing cyber risks. Implementation of the 10 Steps will help organisations reduce the likelihood and cost of a cyber attack or cyber related data breach.

Organisations can also raise their basic defences by enrolling on the Cyber Essentials initiative and following the regularly updated technical guidance on Cyber Security Information Sharing Partnership available on the NCSC website.

Talal Rajab, Head of Cyber and National Security, techUK said: The figures within this report are a welcome indication that efforts to better protect organisations from cyber-attacks through regulation and awareness are having a positive effect. The changes in behaviour due to the introduction of the GDPR is reassuring and we should continue to see an upward curve in data protection amongst UK businesses over the coming years.

However, the report also illustrates that cyber-attacks are becoming increasingly costly to organisations who suffer serious breaches. This is a particularly acute threat to SMEs and charities, many of whom do not have the resources to spend significant sums on cyber products and solutions. We would encourage those organisations to utilise the guidance provided by NCSC and to enrol in schemes like Cyber Essentials to better prepare them for potential attacks.

The full report can be read here: https://bit.ly/2FUuxeM

Data ethics and artificial Intelligence

EP STOA - A governance framework for algorithmic accountability and transparency

Transparency and accountability are both tools to promote fair algorithmic decisions by providing the foundations for obtaining recourse to meaningful explanation, correction, or ways to ascertain faults that could bring about compensatory processes. The study develops policy options for the governance of algorithmic transparency and accountability, based on an analysis of the social, technical and regulatory challenges posed by algorithmic systems.

Based on an extensive review and analysis of existing proposals for governance of algorithmic systems, the authors propose a set of four policy options each of which addresses a different aspect of algorithmic transparency and accountability: (1) Awareness raising: education, watchdogs and

whistleblowers; (2) Accountability in public sector use of algorithmic decision-making.(3). Regulatory oversight and Legal liability and (4) Global coordination for algorithmic governance.

Study; **Annex 1**

US – ARF Adopts Code of Conduct

US based ARF (Advertising Research Foundation) adopted its first member code of conduct on ethical research and data collection. The code outlines general responsibilities for member companies and sector-specific principles for research and data collection.

ARF members include agencies, marketers, media companies, academics and consultants. The organisation plans to enforce the code through a self-regulating programme called the 'Chain of Trust', which will enable members who commit to the principles to display an ARF code logo. Where possible, members will also agree to use suppliers, agencies and adtech third parties who have committed to the code's values.

The code's sector-specific principles are that:

Members should support and/or conduct custom or shared research to determine whether consumers understand the member's terms of service and data privacy policy

Members should state when and how they used automated decision or artificial intelligence systems and provide a clear and easy opt-out ability from this

Researchers provide consumers with an easy way to withdraw consent for the collection and use of their data and that members not make any attempts to influence the accuracy of syndicated media research or syndicated sales or consumer data

Members using location data for research should identify on their website what sources of data are used and provide those targeted with the ability to opt-out of future contacts.

The ARF has built upon existing legislation, regulation and codes including GDPR, CCPA, COPPA and HIPAA. The code reinforces Digital Advertising Alliance guidelines on data privacy, the Neuromarketing Science and Business Association code for the application of neuroscience in business, and ESOMAR and Insights Association codes of standards and ethics for market research and data analytics.

Source: Research Live

URL: https://www.research-live.com/article/news/arf-creates-member-code-of-conduct/id/5052102