

## **Monitoring Report – 25 /01/2019 (No. 2 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.***

### *Regulatory investigations and enforcement*

*Fine of €50 million imposed on Google by CNIL (the French data protection supervisor) made all the headlines this week. Key takeaways from this judgment for research suppliers is the regulatory focus on meeting the GDPR consent standard and fulfilling expectations on the transparency principle. Part of the underlying reason for the fine is that although Google required users to “agree” to its privacy policy in order to use its services, complex and lengthy privacy notices such as Google’s, are not easily understood by individuals. Bundled consents for different purposes means organisations can end up not getting proper consent for any of the purposes. Important that suppliers across the research supply chain properly reflect this in documentation provided to research participants.*

### *Regulatory guidance*

*At the European Data Protection Board (EDPB) recent plenary meeting, guidelines on certification were finalised. Other issues discussed included the Privacy Shield, Brexit, clinical trials Q&A, DPIA lists, EDPB answer to Australian supervisory authority on data breach notification.*

### *Policy developments and legislative initiatives*

*The EU and Japan mutual Data Adequacy agreement created the largest area for data transfers. The European Commissioner Věra Jourová and Commissioner Haruhi Kumazawa welcomed the decisions recognising each other's personal data protection system as equivalent. In other legislative developments the European Parliament LIBE Committee has considered its draft recommendation (consent) on the draft Council decision authorising Member States to ratify, in the interest of the European Union, the modernised Council of Europe Convention 108.*

### *Research and data ethics*

*More developments in ethics and artificial intelligence with the announcement by Facebook of a new partnership with the Technical University of Munich (TUM) to support the creation of an AI ethics research center. The Institute for Ethics in Artificial Intelligence, will be supported by an initial funding grant from Facebook of \$7.5 million over five years, to help advance the growing field of ethical research on new technology and explore fundamental issues affecting the use and impact of AI. The Council has published its Draft Conclusions on the Coordinated Plan on the development and use of Artificial Intelligence Made in Europe.*

## **Regulatory investigations and enforcement**

### ***CNIL fines Google for GDPR breaches***

France's Data Protection Authority, the CNIL, announced a 50 million euro fine on Google LLC for lack of transparency, inadequate information and lack of valid consent regarding the personalisation of advertisements.

The case was initiated by two associations, None Of Your Business ("NOYB") and La Quadrature du Net ("LQDN"). LQDN was supported by 10 000 people to refer the matter to the CNIL. The CNIL says that the GDPR "one-stop-shop mechanism" was not applicable as the DPAs consider that Google did not have one main establishment in the European Union.

The CNIL is of the view that the consents collected were neither "specific" nor "unambiguous". When an account is created, the user can admittedly modify some options associated with the account by clicking on the button "More options" accessible above the button "Create Account". It is possible to configure the display of personalised ads, the CNIL says.

The CNIL continues: "That does not mean that the GDPR is respected. Indeed, the user not only has to click on the button 'More options' to access the configuration, but the display of the ads personalisation is moreover pre-ticked. However, as provided by the GDPR, consent is 'unambiguous' only with a clear affirmative action from the user (by ticking a non-pre-ticked box for instance). Finally, before creating an account, the user is asked to tick the boxes "I agree to Google's Terms of Service" and "I agree to the processing of my information as described above and further explained in the Privacy Policy" in order to create the account. Therefore, the user gives his or her consent in full, for all the processing operations purposes carried out by GOOGLE based on this consent (ads personalisation, speech recognition, etc.). However, the GDPR provides that the consent is "specific" only if it is given distinctly for each purpose."

This fine is the first imposed by the CNIL under the GDPR and it warns that as the infringement is continuing, and it also involves the Android mobile operating system, further sanctions are on the agenda: "It is not a one-off, time-limited, infringement."

Available in French here: **[La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC](#)**

Source: Privacy Laws & Business

## **Regulatory guidance**

### ***EDPB report on the Sixth Plenary session: Privacy Shield, Brexit, clinical trials Q&A, DPIA lists, guidelines on certification, EDPB answer to Australian SA on data breach notification***

On January 22nd and 23rd, the European Data Protection Authorities, assembled in the European Data Protection Board, met for their sixth plenary session. During the plenary a wide range of topics were discussed.

#### **Privacy Shield**

The Board Members adopted the EDPB's report on the Second Annual Review of the EU-US Privacy Shield. The EDPB welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions, as well as the efforts to publish a number of important documents, in part by declassification (such as decisions by the FISA Court), the appointment of a new Chair as well as of three new members of the Privacy and Civil Liberties Oversight Board (PCLOB) and the recently announced appointment of a permanent Ombudsperson.

In view of the findings of the second joint review, the following concerns about the implementation of the Privacy Shield still remain. This includes concerns already expressed by the EDPB's predecessor WP29 on the lack of concrete assurances that indiscriminate collection and access of personal data for national security purposes are excluded. Also, based on the information provided so far, the EDPB cannot currently consider that the Ombudsperson is vested with sufficient powers to remedy non-compliance. In addition, the Board points out that checks regarding compliance with the substance of the Privacy Shield's principles are not sufficiently strong.

Moreover, the EDPB has some additional concerns with regard to the necessary checks to comply with the onward transfer requirements, the scope of meaning of HR Data and the recertification process, as well as to a list of remaining issues raised after the first joint review which are still pending.

#### **Brexit**

The EDPB discussed possible consequences of Brexit in the area of data protection. Members agreed to cooperate and exchange information regarding their preparations and the tools available to transfer data to the UK, once the UK will no longer be part of the EU.

#### **Clinical trials Q&A**

Following a request from the European Commission (DG SANTE), the EDPB adopted its opinion on the clinical trials Q&A. The opinion addresses in particular the aspects related to the adequate legal bases in the context of clinical trials, and the secondary uses of clinical trial data for scientific purposes. The opinion will now be transmitted to the European Commission.

## **DPIA lists**

The EDPB adopted opinions on the Data Protection Impact Assessment (DPIA) lists, submitted to the Board by Liechtenstein and Norway. 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 22 opinions adopted during the September plenary, and the four opinions adopted during the December plenary, and will further contribute to establishing common criteria for DPIA lists across the EEA.

## **Guidelines on certification**

The EDPB adopted the final version of the guidelines on certification following public consultation. Additionally, the Board also adopted a new annex. A draft version of the guidelines had been adopted during the EDPB's first plenary in May. The primary aim of these guidelines is to identify overarching criteria which may be relevant to all types of certification mechanisms issued in accordance with art. 42 and art. 43 GDPR. As such, the guidelines explore the rationale for certification as an accountability tool, provide explanations for the key concepts of the certification provisions in art. 42 and art. 43, explain the scope of what can be certified and outline the purpose of certification. The guidelines will help Member States, supervisory authorities and national accreditation bodies (NAB) when reviewing and approving certification criteria in accordance with art. 42 and art. 43 GDPR. The annex will be subject to public consultation.

## **Response to Australian Supervisory Authority on data breach notification**

In October 2018, the EDPB Chair received a written request from the Office of the Australian Information Commissioner regarding the publication of the data breach notifications by supervisory authorities. The EDPB welcomes the Australian Commissioner's interest in cooperating with the European Data Protection Board on this issue and stresses the importance of international collaboration. In its response, the EDPB provides further information on whether and how supervisory authorities handle the publication of information regarding data breach

## **Policy developments and legislative initiatives**

### ***EU-Japan Data Transfers - Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows***

The Commission has adopted today its adequacy decision on Japan, allowing personal data to flow freely between the two economies on the basis of strong protection guarantees.

This is the last step in the procedure launched in September 2018, which included the opinion of the European Data Protection Board (EDPB) and the agreement from a committee composed of representatives of the EU Member States. Together with its equivalent decision adopted today by Japan, it will start applying as of today.

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality said: "This adequacy decision creates the world's largest area of safe data flows. Europeans' data will benefit from high privacy standards when their data is transferred to Japan. Our companies will also benefit from a privileged access to a 127 million consumers' market. Investing in privacy pays off; this arrangement will serve as an example for future partnerships in this key area and help setting global standards."

The key elements of the adequacy decision

Before the Commission adopted its adequacy decision, Japan put in place additional safeguards to guarantee that data transferred from the EU enjoy protection guarantees in line with European standards. This includes:

A set of rules (Supplementary Rules) that will bridge several differences between the two data protection systems. These additional safeguards will strengthen, for example, the protection of sensitive data, the exercise of individual rights and the conditions under which EU data can be further transferred from Japan to another third country. These Supplementary Rules will be binding on Japanese companies importing data from the EU and enforceable by the Japanese independent data protection authority (PPC) and courts.

The Japanese government also gave assurances to the Commission regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms.

A complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority.

The adequacy decisions also complement the [EU-Japan Economic Partnership Agreement](#) - which will enter into force in February 2019. European companies will benefit from free data flows with a key commercial partner, as well as from privileged access to the 127 million Japanese consumers. The

EU and Japan affirm that, in the digital era, promoting high privacy and personal data protection standards and facilitating international trade must and can go hand in hand.

#### Next steps

The adequacy decision – as well as the equivalent decision on the Japanese side – will start applying as of today. After two years, a first joint review will be carried out to assess the functioning of the framework. This will cover all aspects of the adequacy finding, including the application of the Supplementary Rules and the assurances for government access to data. The Representatives of European Data Protection Board will participate in the review regarding access to data for law enforcement and national security purposes. Subsequently a review will take place at least every four years.

#### Background

The mutual adequacy arrangement with Japan is a part of the EU strategy in the field of international data flows and protection, as announced in January 2017 in the [Commission's Communication on Exchanging and Protecting Personal Data in a Globalised World](#) .

The EU and Japan successfully concluded their talks on reciprocal adequacy on 17 July 2018 (see [press release](#) ). They agreed to recognise each other's data protection systems as adequate, allowing personal data to be transferred safely between the EU and Japan.

In July 2017, President Juncker and Prime Minister Abe committed to adopting the adequacy decision, as part of the EU and Japan's shared commitment to promote high data protection standards on the international scene (see [statement](#) ).

The processing of personal data in the EU is based on the [General Data Protection Regulation](#) (GDPR), which provides for different tools to transfer personal data to third countries, including adequacy decisions. The European Commission has the power to determine whether a country outside the EU offers an adequate level of data protection. The European Parliament and the Council can request the European Commission to maintain, amend or withdraw these decisions.

#### For More Information

[The adequacy decision and related documents](#)

[Factsheet on the EU-Japan Adequacy Decision](#)

[Press release on launch of the adoption procedure](#) (5 September 2018)

[Press release on the conclusions of the adequacy talks](#) (17 July 2018)

[Questions & Answers on the Japan adequacy decision](#)

[Statement](#)

## *ePrivacy Regulation developments*

FEDMA reported that the Rumanian Presidency is aiming to reach an agreement on the [ePrivacy file](#) within the next 5 month, and has scheduled a series of meeting of the working party on telecommunication and information society, in January where attaches from each Member States discuss the remaining open issue of the text. Amongst the issues that still remain open are related to security, confidentiality of communication browser settings and cookie walls and the direct marketing provision.

## *Debate on report on Modernised Council of Europe Convention*

On January 23, the European Parliament LIBE Committee held a consideration of its draft recommendation (consent) on the draft Council decision authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Press Release from the European Commission on the publication of the report on the second annual review of the functioning of the EU-U.S. Privacy Shield.

**József Nagy (EPP, SK), rapporteur** , was of the view that the modernised Council of Europe Convention 108 is in line with the EU data protection model and legislation. He noted that the amending protocol was prepared in parallel with the European data protection reform package in order to ensure consistency between the instruments. As such, the Convention mirrors the Union data protection legislative framework, such as the GDPR and the Police-Directive. Convention 108 plays a crucial role in spreading the 'European data protection model' globally as it is often used as a source of inspiration by countries which consider adopting new privacy legislation or harmonising privacy law with international standards. Moreover, a higher level of protection will facilitate the exchange of personal data based on appropriate safeguards. Increasing the data protection standards of the Convention will also facilitate data flows between the EU and the non-EU Parties to the Convention. The amending protocol introduces the possibility for the Union and other international organisations to become a Party to the Convention 108.

**Romeo Franz (Greens/EFA, AT), shadow** , stated that here is case of EU legislation which, when done properly, can be an example for the world. Convention 108 inspired the EU Data Protection Directive adopted in 1995 and now it was the other way around. In addition, due to the involvement in the Council of Europe of countries outside the EU, this means that the GDPR will also have an effect in the wider world.

The ratification of the revised Convention 108 is therefore something to be supported. MEP Franz further noted that California has also adopted a comprehensive data protection law.

**The European Commission representative** was of the view that this an important instrument for the EU but that also goes beyond the EU, as 53 parties are involved. There are participating parties in Africa and in Latin America and some observers are from Asia. He noted that the U.S., who is



currently pushing for an alternative model with a lower standard of protection – the APEC Privacy Framework – was also encouraged to join Convention 108 in the recent review of the EU-U.S. privacy shield. The representative then underlined the importance of ensuring the ratification of Convention 108, as it can only enter into force after 38 ratifications. Presently, he noted, 10 EU member States have not even signed the Convention. He thus called on the Parliament to join the Commission in encouraging Member States to sign this instrument

## **Research and data ethics**

### ***Facebook and the Technical University of Munich Announce New Independent TUM Institute for Ethics in Artificial Intelligence***

Facebook announced a new partnership with the Technical University of Munich (TUM) to support the creation of an independent AI ethics research center. The Institute for Ethics in Artificial Intelligence, which is supported by an initial funding grant from Facebook of \$7.5 million over five years, will help advance the growing field of ethical research on new technology and will explore fundamental issues affecting the use and impact of AI.

Artificial intelligence offers an immense opportunity to benefit people and communities around the world. But as AI technology increasingly impacts people and society, the academics, industry stakeholders and developers driving these advances need to do so responsibly and ensure AI treats people fairly, protects their safety, respects their privacy, and works for them.

At Facebook, ensuring the responsible and thoughtful use of AI is foundational to everything we do – from the data labels we use, to the individual algorithms we build, to the systems they are a part of. We're developing new tools like [Fairness Flow](#), which can help generate metrics for evaluating whether there are unintended biases in certain models. We also work with groups like the [Partnership for AI](#), of which Facebook is a founding member, and the [AI4People initiative](#). However, AI poses complex problems which industry alone cannot answer, and the independent academic contributions of the Institute will play a crucial role in furthering ethical research on these topics.

The Technical University of Munich is one of the top-ranked universities worldwide in the field of artificial intelligence, with work extending from fundamental research, to applications in fields like robotics and machine intelligence, to the study of the social implications of AI. The Institute for Ethics in Artificial Intelligence will leverage the TUM's outstanding academic expertise, resources and global network to pursue rigorous ethical research into the questions evolving technologies raise.

The Institute will also benefit from Germany's position at the forefront of the conversation surrounding ethical frameworks for AI – including the creation of government-led ethical guidelines on autonomous driving – and its work with European institutions on these issues.



## **Institute Overview**

Drawing on expertise across academia and industry, the Institute will conduct independent, evidence-based research to provide insight and guidance for society, industry, legislators and decision-makers across the private and public sectors. The Institute will address issues that affect the use and impact of artificial intelligence, such as safety, privacy, fairness and transparency.

Through its work, the Institute will seek to contribute to the broader conversation surrounding ethics and AI, pursuing research that can help provide tangible frameworks, methodologies and algorithmic approaches to advise AI developers and practitioners on ethical best practices to address real world challenges.

To help meet the need for thoughtful and groundbreaking academic research in these areas, Facebook looks forward to supporting the Institute and help offer an industry perspective on academic research proposals, rendering the latter more actionable and impactful.

## **Operational Model**

The independent Institute will be led by TUM Professor Dr. Christoph Lütge, who holds degrees in business informatics and philosophy and has served as the Peter Löscher Endowed Chair of Business Ethics at TUM since 2010. Working with a diverse advisory board of representatives from academia, civil society and industry, the Institute will identify specific research questions and convene researchers focused on AI ethics and governance-related issues.

"At the TUM Institute for Ethics in Artificial Intelligence, we will explore the ethical issues of AI and develop ethical guidelines for the responsible use of the technology in society and the economy," Dr. Lütge said. "Our evidence-based research will address issues that lie at the interface of technology and human values. Core questions arise around trust, privacy, fairness or inclusion, for example, when people leave data traces on the internet or receive certain information by way of algorithms. We will also deal with transparency and accountability, for example in medical treatment scenarios, or with rights and autonomy in human decision-making in situations of human-AI interaction."

While Facebook has provided initial funding, the Institute will explore other funding opportunities from additional partners and agencies. Facebook may also share insights, tools, and industry expertise related to issues such addressing algorithmic bias, in order to help Institute researchers focus on real-world problems that manifest at scale.

The Institute will also pursue opportunities to publish research and work with other experts in the field; organize conferences, symposia, and workshops; and launch educational activities with other leading institutions in common areas of interest.

Realizing AI's huge potential for good while balancing its risks is a global effort, and it will not be accomplished overnight. The Institute is an exciting step forward in our continued commitment to partnering with academic institutions, governments, NGOs, advocacy and industry groups, and others who are working to advance AI in a safe and responsible way.

### ***Draft Conclusions on Co-ordinated Plan on development and use of artificial intelligence made in Europe***

The Council has published its Draft Conclusions on the Coordinated Plan on the development and use of [Artificial Intelligence Made in Europe](#).

### ***EU Parliament Briefing on Artificial intelligence: the challenges for EU citizens and consumers***

The EU Parliament published a briefing “[Artificial Intelligence: the challenges for EU citizens and consumers](#)”. The briefing addresses the regulation of artificial intelligence (AI), namely, how to ensure that AI benefits citizens and communities, according to European values and principles. Focusing on data and consumer protection, it presents risks and prospects of the applications of AI, it identifies the main legal regimes that are applicable, and examines a set of key legal issues.

## ***Upcoming Events***

### ***January 2019***

#### ***CPPD 2019 Data Protection and Democracy***

30 January to 1<sup>st</sup> February 2019, Brussels, Belgium

CPDP is an annual three-day conference devoted to privacy and data protection. The overarching theme of the 2019 edition is “Data Protection and Democracy”. The entwinement between data analytics and democratic processes has been on the spotlight for the better part of the past two years.

URL: <https://www.cdpconferences.org/call-for-papers>

### ***March 2019***

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

20 March 2019, Brussels, Belgium

***The Annual European Data Protection and Privacy Conference will return to Brussels in Spring 2019. Gathering over 200 cross-sector delegates and attracting an impressive line-up of top-level speakers every year, this event has become the must-attend annual data protection and privacy conference held in Brussels.***

**We are delighted to announce that Commissioners Věra Jourová and Mariya Gabriel will join us as a keynote speakers at the event.**

2018 was a pivotal year for data protection and privacy in both the EU and globally. 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](#)