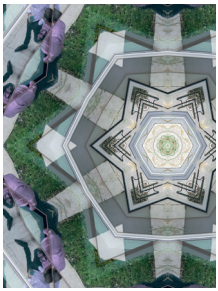
ARTHUR COX

DATA PROTECTION &
INFORMATION MANAGEMENT

EU Regulatory Update and Horizon Scanning

EU Privacy Perspective, February 2020



REGULATORY UPDATE

Recent fines imposed

Italy

In January, Italy's Garante imposed an €8.5 million fine on a utility provider for GDPR violations in connection with telemarketing and promotional phone calls without consent, impacting approximately 7,200 customers.

Greece

In December 2019, a Greek company was fined €150k (circa. US$160k) for several GDPR violations, including the fact that several external companies had access to and were able to copy personal data from its servers due to the controller's failure to implement adequate security measures.

Spain

Spain's AEPD has been actively enforcing in recent times including imposing fines of: €3k for failing to provide requested information to the regulator in time; €44k for inadvertently sending consumer contracts to wrong recipients; and €75k for processing data without a valid lawful basis.

UK

The UK's Information Commissioners Office ("ICO") also fined a London-based pharmacy £275k (circa. US€358k) for failing to ensure security of medical data after the company had left approx. 500,000 documents (including names and prescriptions) in unlocked containers in the back of its premises.

Cracking the children's code

Policy debate

In November 2019, FTC Commissioner Rebecca Slaughter, Irish Data Protection Commissioner Helen Dixon and the UK ICO's Simon McDougal examined children's privacy on a panel in Brussels. Unsurprisingly, the panel expressed a preference for contextual advertising to children over targeted ads (based on profiling). Commissioner Slaughter also called for suicide and self-harm issues to be part of this wider discussion and noted the huge potential for the development "kid-tech" solutions for many privacy issues.

UK

The UK's ICO has since released an "Age Appropriate Design Code" in January 2020: if approved by parliament, the Code will be binding on online services "likely to be accessed by children" in the UK, which will be required to have "high privacy" settings by default (i.e. by turning off location tracking, not using nudging techniques, etc.).

Ireland

Similarly in Ireland, the DPC has conducted a public consultation on the processing of children's data throughout 2019, producing two reports. In terms of next steps, the DPC has stated that it will engage with industry stakeholders in the first half of 2020 (in particular large technology platforms) to encourage a code of conduct on children's data, as the DPC is mandated to do under the Irish Data Protection Act 2018.

AG opinion on law enforcement disclosure

In January 2020, the Advocate General in Case C-623/17 found that the disclosure of "bulk" communications data by mobile network operators to UK law enforcement agencies could not be automatically justified on grounds of safeguarding "*national security*" under the ePrivacy Directive. The notion of national security must be "*interpreted narrowly*", which the AG found will not be the case where "*it involves general and indiscriminate retention of personal data*". While not binding on the CJEU, the EU's highest court typically follows the AG's opinion and it remains to be seen how the court will rule in this important case.

Over the top and into scope?

While GDPR remains the chief focus, privacy lawyers have also been keeping one eye on the ePrivacy Regulation, but the introduction of the European Electronic Communications Code ("**EECC**") has been comparatively low key. With effect from December 2020, the EECC will introduce legislative changes which will bring providers of "interpersonal communications services" within scope of the ePrivacy Directive. This means that so-called "over-the-top" (or OTT) services, such as VoIP and web-based email and messaging services, will for the first time be subject to communications content and traffic data confidentiality obligations and interception prohibitions under existing law. Importantly this change will take effect *before* the ePrivacy Regulation is introduced (see below).

The ePrivacy Regulation saga continues...

Initially published in January 2017, with the ambitious aim of accompanying the GDPR into force on 25 May 2018, the proposed ePrivacy Regulation has met many obstacles as it slowly navigates through the EU legislative process. The proposed new law will govern cookies, direct marketing and confidentiality of communications via both traditional telecommunications and online communications services (including OTT services).

The negotiating stumbling blocks have centred on the issue of ensuring the confidentiality of communications, the safeguards required and what, if any, exceptions should be permitted (one central issue being the extent to which child exploitation content can be filtered).

The next draft of the proposed Regulation is expected to be published later in February 2020 by the Croatian Presidency of the Council of the EU, and should this attempt fail to bear fruit, Germany will assume responsibility once it assumes the rotating 6-month Council presidency in July 2020. It could well be the case that the draft law makes significant legislative progress during the second half of 2020.

Shortening the long arm of the GDPR: territoriality guidance

The European Data Protection Board ("**EDPB**")'s final guidance on the GDPR's territorial scope (published in November 2019), sheds further light on the following issues:

Processing "activities" not organisations

In assessing whether the GDPR applies, an organisation should analyse whether specific "processing activities" are in scope rather than the organisations itself. Consequently, one set of processing activities may be in scope while another – undertaken by the same organisation – may not be.

Non-EU controllers

The EDPB clarified that the GDPR will not apply to a controller solely because it uses a processor or vendor established in the EU.

Intention rather than inadvertent targeting

Sensibly, EDPB also made clear that the GDPR applies to processing activities that "*intentionally, rather than inadvertently or incidentally, target individuals in the EU*" for the purposes of offering goods and service to them.

Cookies and AdTech: a recipe for uncertainty

In 2019 no less than six EU supervisory authorities published guidance on cookies compliance: an area that individual member states retain discretion to set their own rules within the parameters of the ePrivacy Directive. The often divergent regulatory guidance has introduced an element of uncertainty as to the permissibility of cookie paywalls and consent requirements for analytic cookies, to name but two issues. Introduce AdTech to the mix and challenges around transparency and collection of consent, as separately identified in detailed papers by the ICO and France's CNIL, mean that the AdTech model will require substantial re-configuration to survive 2020.

HORIZON SCANNING

What to expect in 2020 and beyond

EU Face-off with AI

A recently leaked European Commission white paper indicates EU plans to regulate AI. According to the document, the proposed measures may include a light-touch voluntary labelling system for "trustworthy-AI", regulation limited to public bodies, and risk-based regulation targeting AI applications perceived as "higher risk". The paper also considers a temporary ban on the use of facial recognition technology in public spaces (for a period of 3-5 years), during which the impacts of AI technology can be assessed and suitable risk management measures developed. Further official updates on these proposals are expected through Spring 2020.

EDPB role in Merger Control?

Arising from Google's proposed £2.1 billion acquisition of Fitbit, several EU data protection authorities have backed a proposal to review the data protection implications of the transaction at EDPB level and to submit their findings to the European Commission, the body responsible for merger control / regulatory approval in the EU.

Irish DPC's enforcement priorities

The DPC has launched a public consultation on its Regulatory Strategy 2020-2025 with the stated purpose of providing "*insight and greater certainty to organisations and people on how the DPC intends to regulate to maximum effect*". The DPC has separately identified private sector processing of health and genetic data for commercial purposes and connected cars as priority enforcement areas in 2020 and beyond.

Irish focus

Formulaic fining methodology dismissed

In October 2019, the German DPAs together published fining guidelines under GDPR, containing prescriptive rules on how fines should be calculated. The Irish DPC has dismissed the guidelines as "premature", insisting that each case must be assessed on its merits and that any fines must have a "rational basis" in law (rather than a strict formula).

Digital assistants

Appearing before an Irish parliamentary committee on voice-enabled digital assistants in late 2019, the Irish DPC made the following statements:

- "*Human review of voice data collected and processed by automated means is a common method to review, improve and train the algorithms used in voice assistant technology. While not inherently problematic or contentious from a data protection perspective, this kind of processing has many data protection elements, which must be carefully considered and assessed by the companies providing such services to ensure that the use of user data is legitimate and appropriately protected.*
- On transparency and awareness: "*...we are used to dealing with keyboards and computers* [compared] *to in-home devices where our voices are being processed, where the processing is sometimes invisible or it could be said to be that because it is going on in the background. It is ambient. That changes the way we interact with these things and it changes our expectations as well.*"

Data protection-by-design a top priority

In November 2019, the EDPB published draft guidance on data protection-by-design (still open for public consultation), in which the Irish DPC acted as co-rapporteur. The DPC commented as follows:

- "*Article 25 of the GDPR imposes a legal obligation on data controllers, the organisations that create these devices and do the processing, to account for data protection by design in everything they do. It is not just about ... data minimisation or security. It is to do with transparency and the legal basis for how they gather consent, the way they process data, the way they design their processing chain from start to finish...*".

This is particularly pertinent in light of recent comments by Helen Dixon to the effect that data protection compliance needs to "*move beyond first principles*".

Our data protection team

Rob Corbet
Head of Data Protection and Information Management
+353 1 920 1211
rob.corbet@arthurcox.com

Olivia Mullooly
Partner
+353 1 920 1060
olivia.mullooly@arthurcox.com

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Hugh McCarthy
Associate
+353 1 920 1324
hugh.mccarthy@arthurcox.com

Ciara Anderson
Associate
+1 415 829 4247
ciara.anderson@arthurcox.com

Ian Duffy
Associate
+353 1 920 2035
ian.duffy@arthurcox.com

Colm Maguire
Associate
+353 1 920 1416
colm.maguire@arthurcox.com

Caoimhe Stafford
Associate
+353 1 920 1328
caoimhe.stafford@arthurcox.com

Eoghan Clogher
Associate
+353 1 920 1405
eoghan.clogher@arthurcox.com

Aoife Coll
Associate
+353 1 920 1726
aoife.coll@arthurcox.com

Pearse Ryan
Consultant
+353 1 920 1180
pearse.ryan@arthurcox.com

Rachel Benson
Professional Support Lawyer
+353 1 920 1435
rachel.benson@arthurcox.com

Dublin
+353 1 920 1000
dublin@arthurcox.com

Belfast
+44 28 9023 0007
belfast@arthurcox.com

London
+44 207 832 0200
london@arthurcox.com

New York
+1 212 782 3294
newyork@arthurcox.com

San Francisco
+1 415 829 4247
sanfrancisco@arthurcox.com

arthurcox.com