EU Clarifies the European Parameters of Data Protection

Citation for published version:

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Ingenia

Publisher Rights Statement:

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
OPINION: EU CLARIFIES PARAMETERS OF DATA PROTECTION

The European Union’s General Data Protection Regulation, due for adoption this year, is intended to harmonise data protection laws across the EU. Burkhard Schafer, Professor of Computational Legal Theory at the University of Edinburgh, outlines the key points and comments on the engineering implications and legal ramifications of the new regulatory regime.

The growing globalisation of data flows and the ever-increasing capabilities of big data analytics increase the risk that people can lose control of their own data. The new EU regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data is expected to be agreed between the European Commission, Parliament and Council during 2015, aims to strengthen the current situation as one of “fragmentation and incoherence”.

The proposed regulation not only creates new legal rights for citizens; it also gives software developers and hardware engineers a pivotal role in their enforcement. Creative and intelligent design and manufacturing solutions will be needed, including new ways to develop data mining algorithms that offer the same benefits to businesses while collecting less personal data than at present. New ways to build hardware will be needed that, for instance, limit what the sensors of a machine can see without reducing its performance significantly.

A short example can illustrate this point. In 2014, the Court of Justice of the European Union ruled in Google v González that Google was under an obligation to remove links to personal information, at the request of a data subject, provided the information is “inadequate, irrelevant or excessive”. Google’s response to this decision framed it as a trivial issue of data protection compliance: the ruling was a potential interference with its business, to be complied with only up to the degree mandated by law. One consequence, to the dismay of the EU, was to exclude the google.com domain from this process, arguing that the CJEU has no jurisdiction over the US part of its business.

The response could have been very different had Google framed the situation as an engineering challenge. Google’s business is information retrieval (IR). Good IR does not retrieve everything, only information that is relevant, adequate and timely. Framed like this, the decision requires Google to remove only data that a “perfect” IR algorithm would have excluded anyway. “Perfect” IR algorithms are a difficult task – even for AI. Seen like this, Mr González and every engineer can sympathise with Google’s desire to retain its data collection processes. This would also have sidelined the question of jurisdiction.

The new product is better, not just EU law compliant, and thus of benefit for every user worldwide. However, such a gestalt switch that sees Mr González not as a disruptive litigant, but a knowledge engineering resource, requires a new breed of lawyers. Traditionally, lawyers come in only after a data breach has occurred to attribute blame, or after a product is developed to express concerns. Now, they will need to understand enough engineering to suggest creative design and manufacturing solutions as part of harm prevention through technology, working closely with developers. Equally, it requires a new breed of engineers who understand about the law that it becomes for them almost like a material to work with. In other words, the regulation forces engineers and lawyers to work together in new ways to create systems that respect the individual’s right to privacy while allowing new technologies to thrive.

Are we ready in the UK for this revolution in the way we think about the interaction between lawyers and engineers? There are grounds for concern, many with regards to education, curricula design and training. In the US, law degrees are postgraduate qualifications studied after completion of a degree in another field. This produces a much greater pool of lawyers with a background in science and engineering. Germany, by contrast, has its technical universities, powerhouses for technological invention and innovation. Lacking law schools, these universities embed instead individual law academics in informatics or engineering departments. This benefits curriculum design – engineering students will have been exposed at least to some legal training – as well as collaborative research and development.

In the UK, engineering and law departments often have little interaction. Working within these structures to ensure that we prepare the next generation of students for the radically changed legal regime will be a challenge. Professional bodies also have their part to play, not only through their influence on curricula, but also by formulating appropriate standards and supporting them through continued professional development.

The new regulation, rightly used, is an opportunity, not a hindrance. Under its regime, technology-savvy lawyers and legally aware engineers will be worth their weight in gold for technology companies across the world.