Guest Editorial

The EU GDPR as a clarion call for a new global digital gold standard

Giovanni Buttarelli*

The General Data Protection Regulation (GDPR) is going to raise the bar for data protection laws around the world. My EU institution (the Office of the European Data Protection Supervisor, or EDPS) was closely involved—as were other data protection authorities—in the policy discussions, though not in the negotiations.[1] Political agreement was reached in December 2015, and the text is expected to become law before the summer.[2] We believe that we have had some influence over the process, but we do not pretend that the final outcome is perfect, and in some ways it is quite far from the ideal. Nevertheless, we intend to be among the loudest champions of this reform, which is quite simply, and by a long way, the most ambitious endeavour so far to secure the rights of the individual in the digital realm for a generation.

The GDPR contains considerable flexibility, and certainly more than it appears at first sight. It aims to entrench privacy on the ground and allows different sectors to contribute to new norms and best practices appropriate to specific circumstances. Its cornerstone is the notion of trust: trust in data controllers to treat personal information responsibly, and trust that the rules will be effectively enforced. It will be incumbent on Europe's independent data protection authorities, working through a reinforced cooperation facility called the European Data Protection Board, to foster that trust and accountability, by being transparent and accessible to stakeholders and efficient in providing relevant and timely guidance on compliance.

The GDPR will have two major strategic consequences.

The first consequence is that the GDPR sets up a genuine platform for global partnerships. This reflects the global nature of data flows, enabled by technologies and driven by creative, disruptive business models. Over half the countries in the world now have a data protection and/or privacy law, and most are strongly influenced by the European approach, a trend towards the 'global ubiquity' of data privacy.[3] The regulation promises a wider scope for cooperation between authorities and data controllers both within the EU and internationally. It should galvanise efforts for a more consistent standard contractual clauses, speed up the validation process for binding corporate rules, and help them dovetail with similar arrangements elsewhere in the world. I hope that the new provisions for codes of conduct, seals, certification, and accreditation processes will incentivise controllers inside and outside the EU to take the initiative in devising standards which are both business friendly and in the interests of individuals.

The second consequence is that data protection is no longer an optional extra. The Court of Justice of the European Union applies these rules strictly, interpreting them in the light of the EU Charter of Fundamental Rights, and favouring the rights and interests of the individual above corporate or business aims, however reasonable and legitimate. The EU cannot retreat from these core values. Data protection authorities will have to be vigilant in monitoring implementation of the GDPR, and applying the newly amplified range of possible sanctions in case of violation.

Accountability therefore becomes central.[4] This term, which has currency in English but in few other languages, has in fact very ancient roots. The word is

* European Data Protection Supervisor, Brussels.

1 See EDPS Opinion on the Commission's proposed reform package, March 2012: EDPS Opinion 3/2015 (with addendum) 'Europe's big opportunity', EDPS recommendations on the EU's options for data protection reform, July/October 2016.

2 The most up-to-date text reflecting the agreement reached at the political level by the Council and the European Parliament is Council of the European Union document 15039/15, dated 15 December 2015. At the time of writing, this was still subject to checking and translation into the EU's other official languages by lawyer-linguists. The final version will be put to the Council and the European Parliament for adoption, which is expected in May or June 2016, prior to publication in the EU Official Journal.

3 Graham Greenleaf, 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority' (2015) 133 Privacy Laws & Business International Report, February 2015.

4 The concept first appeared in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and was more recently promoted at the 2009 International Conference of Data Protection and Privacy Commissioners in the 'Madrid International Standards', in the ISO draft standard 29100, and in the APEC privacy framework and its cross-border privacy rules. Article 22 of the latest version of the GDPR requires controllers to implement appropriate technical and organisational measures to ensure and demonstrate compliance (the term 'accountability' is defined in Article 5(2)).

derived ultimately from the Latin *putare* meaning 'to reckon'. The concept has been incorporated into data protection because the need for such 'reckoning' stretches across all sectors that handle personal information, including government, private, academia, commercial, and not for profit. There has been an exponential rise in the volumes of personal data being collected, stored, and transferred, which information is increasingly not provided by the individual him- or herself, but rather observed, derived, or computed by someone else. For human rights to have any meaning, it is therefore essential for someone to be responsible for how that data are used. Individuals are subject to granular inferences drawn from statistics through advanced analytics based on algorithms of which they are at best only partially aware. They are put at risk by data processing which is unfair or discriminatory and which entrenches stereotypes and social exclusion. Accountability should promote sustainable data processing, by ensuring that the burden of assessing the legality and fairness of complex processing falls primarily on controllers and regulators, not on the individual.

The EDPS this year is launching a project to explain and start to implement accountability in the way we process personal information across all EU institutions, beginning with our own. We will publish the results of this exercise as a contribution to the understanding of this principle among fellow data protection authorities as well as controllers.

Being accountable for data processing is not a substitute for compliance with the applicable legal obligations. It should be understood as an ethical responsibility for activities that take place for a given purpose, whether profit making, law enforcement, social care, or research—or even a combination of them.

Now is the time to build bridges between the regions of the world on sustainable personal data processing. Bearing in mind that bridges are constructed from two sides with a common goal, we need a robust model for how bilateral data sharing agreements can work. The Safe Harbor agreement did not stand the test of time, so negotiators from the EU and the USA have tried to repair the damage with the proposed Privacy Shield. Europe's data protection authorities are studying this complex document to test its likely longevity.

Similar exercises to that ongoing between the EU and USA may now be needed between other trading partners. My hope is that, during the period of a generation for which the GDPR is likely to apply, we will have achieved a common standard, a sort of digital gold standard, which will accompany globalisation and all the benefits and challenges it poses for individuals and society.

doi:10.1093/idpl/ipw006