Viewpoint

The EU General Data Protection Regulation (GDPR): European regulation that has a global impact

Michelle Goddard

DOI: 10.2501/IJMR-2017-050

significant impact. This strengthening and expansion of EU data protection law presents as an opportunity for privacy-aware and accountable researchers. Researchers steeped in ethical approaches to data collection need to use this as an avenue to build public trust and increase their reach across the data analytics environment.

Introduction

The EU General Data Protection Regulation (GDPR), which will be enforced across all EU Member States from 25 May 2018, is a landmark in the evolution of the European privacy framework.[1] Driven by a philosophical approach to data protection, based on the concept of privacy as a fundamental human right (as enshrined in the Charter of EU Rights), the Regulation will have wide global impact.

The new law covers the personal data of all EU residents, regardless of the location of the processing. Personal data is information that, directly or indirectly, can identify an individual, and specifically includes online identifiers such as IP addresses, cookies and digital fingerprinting, and location data that could identify individuals. This is much wider than the concept of personally identifiable information under US privacy law.

The wide territorial scope and expanded definitions of personal data ensure that the GDPR will have a

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Core privacy principles

The GDPR has six general data protection principles (fairness and lawfulness; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality) but data protection by design and default is at the core of the GDPR. It is supported on one side by transparency (through ensuring full information is provided to individuals in an accessible style and manner) and on the other side by accountability (ensuring that all organisations take demonstrable responsibility using personal data).

Operationalising and enshrining these principles in the research cycle requires proactive design and conceptualisation of privacy as the default for any data collection exercise. It also needs to be embedded both in the design systems of any IT architecture and general organisational business practices of research agencies and clients.

Accountability requires organisations to put in place appropriate technical and organisational measures, and to be able to demonstrate what they did and its effectiveness when requested. This may also include the

use of privacy impact assessments for high-risk processing. GDPR also introduces a mandatory data breach notification regime.

A key change to note in lawful processing is the standard required for consent. GDPR consent must be freely given, specific, informed and evidenced by clear affirmative action. It must also be verifiable, with a higher standard of explicit consent required to process sensitive data.

Processing of data is fair only if it is transparent and this means there must be openness in data processing through effective communication with individuals including in the use of information notices. GDPR is user-centric, so transparency in a GDPR context means a move away from legal tick-box compliance to a tailored, reflective and dynamic approach. Extensive information must be provided to individuals including details about recipients, retention periods and the range of their individual rights such as access and portability. All of this needs to be provided in an accessible language to ensure that it can easily be understood.

Wide jurisdictional scope

The long-arm jurisdictional reach of the Regulation is one of the key innovations as it covers organisations without an EU presence that target or monitor EU individuals. Organisations subject to this must appoint an EU-based representative. It remains to be seen how effective compliance against overseas-based organisations will be. It is likely that, in these types of cases, the EU-based regulator will work with the regulator based in the third country, and enforcement activity will be tempered both by enforcement priorities and the increased overall volume of work arising from the new framework.

Organisations based outside the EU will also face pressure for GDPR compliance as part of the supply chain for research services. Clients using data processors based outside the EU will need to ensure that the higher GDPR standards are reflected in the contractual provisions. This may lead to more detailed supplier questionnaires and greater auditing of the business. Negotiations around apportionment of liability can also be expected to play a larger part of the contracting process.

Challenges remain

The current data protection framework, implemented through an EU Directive, has led to divergent interpretations in the Member States. One of the major changes with the new framework is that, as a Regulation, it is directly applicable, with limited scope for Member States to impose their own rules. Consistency of enforcement will be aided by the establishment of the European Data Protection Board, consisting of the supervisory authorities from all the Member States that will issue guidance, work towards uniformity of enforcement proceedings and determine disputes involving processing in more than one Member State.

Uncertainties remain, however, as the GDPR has scope for states to use the legislative derogations (flexibilities) to create different rules in a range of areas such as the age that children can consent to online information services, the allowable legal grounds for processing sensitive personal data and the require-

ments for mandatory appointment of a data protection officer. The application of the special research regime, which provides certain flexibilities for scientific and statistical research (including relaxation of several individual rights), is also subject to Member State action. One unifying thread is that pseudonymisation must become the default for all research projects, and clear ethical and organisational measures put in place.

Guidance has been issued by EU regulators and there is a rolling programme that will assist in future interpretation of the GDPR on areas such as transparency and international data transfers. However the EU data protection project is not yet complete. The final content of the ePrivacy regulation – unlikely before spring 2019 – will impact on the online environment.

But opportunities abound …

In the words of the UK Information Commissioner's Office, 'GDPR is an evolution in data protection, not a burdensome revolution.'[2] Nevertheless it marks a fundamental change in the balance of power between organisations and individuals in the collection, processing and storage of personal data elevating individuals' right to access and control use of their personal data.

GDPR goes beyond current law in demanding higher standards for organisations processing data – but these higher standards are philosophically in line with best practice and ethical approaches that are practised by research practitioners. Organisational measures must be more effective and embedded throughout the organisation, but GDPR builds on transparency and trust enshrined in national and international codes with best practices that put the interests of research participants rightfully at the centre.

Michelle Goddard
Director of Policy and Standards, MRS, and Director of Policy and Communications, EFAMRO

[2] ICO blog, 25 August 2017.