THE OFFICE OF THE
Data Protection Authority

The GDPR two years on: doing the right thing with data

By Christopher Docksey
(Member of The Data Protection Authority)

THE OFFICE OF THE Data Protection Authority

We live in the ever-accelerating technology age of big data, cloud computing, the Internet of Things, AI, and facial recognition.

We are increasingly sharing, and being required to disclose, our personal information, over the Internet and as we move around in public. 'Big Data' combines the huge volumes of information about our interests, relationships, location, race, religion, political views, gender, sexuality, and health, and analyses them to give powerful insights.

There is no doubt that these new technologies will deliver significant benefits for our economies and our everyday lives.

For example, the smartphone apps presently being developed will be able to assist human tracking and tracing in combatting COVID-19. Big data analytics has the potential of improving policies in a wide range of areas.

But there is a cost. We learned from the Cambridge Analytica scandal that our personal information can be used not only to monitor our behaviour but also to predict and even to influence what we do.

As Bruce Schneier said: '**If something is free, you're not the customer, you're the product.**'

The development of artificial intelligence makes it possible for companies to create digital profiles, to share them in microseconds without our knowledge, and use them as the basis for important decisions about us. As a result, despite the fact that data protection is a fundamental right under the **EU Charter of Fundamental Rights**, such monitoring and profiling has become the internet's prevailing business model.

These are the roots of the GDPR. As well as the development of intrusive surveillance tools, we are threatened by identity theft, leaks of sensitive data, discrimination and in-built bias, and sharing of illegal content. The data protection rules had to be updated. We needed to facilitate responsible data processing to preserve our good human values, to protect our privacy and our secrets, and to allow us to freedom to develop our personalities and our relationships.

Big Data needed equally big Data Protection.

This was easier said than done. Big Data fought back.

It took three years of preparation followed by four years of intense legislative discussions to adopt the GDPR. It became one of the top two most heavily lobbied pieces of EU legislation ever, with **a record 3,999 amendments** to the European Parliament's text.

However the GDPR was finally adopted on 27 April 2016, subject to a two year grace period before it entered into application on 25 May 2018.

On that day it became law in the then 28 EU Member States; it was adopted into national legislation in the three EEA States of Norway, Iceland and Liechtenstein; and *The Data Protection (Bailiwick of Guernsey) Law, 2017* came into force in Guernsey.

The rules on data protection are based on three fundamental suppositions.

- First, **data protection is intended to facilitate processing**, not to stop it.
  The data protection rules are designed to support the processing of personal information by laying down the *rules of the road*. Because the law in the Bailiwick respects the same legal standards as the GDPR, an EU 'adequacy' decision entitles Guernsey businesses to transfer personal information between the island and the EU freely and without any extra bureaucratic requirements. Digital flows are now so important for the island's economic growth that this favourable status gives Guernsey businesses a significant advantage over companies in other countries which trade and interact with the EU.
- Second, **the success of the information society has to be based on trust**.
  Consumers can be uneasy about how their personal information is handled by companies and public authorities, so trust is essential if people are to consume digital services. We can see this very clearly in the debate on devising tracking apps to help combat COVID-19. Individuals are much more likely to download and use an app if the system is based on transparency, trust and high privacy protection.
- Third, **technology is there to *serve* us**, not *dictate* to us.
  The GDPR declares that the processing of personal data *should be designed to serve mankind*. We need to think hard not only about the legal but also the ethical implications of current technological trends for our personal dignity and individual freedom.

The main innovations in the GDPR and the 2017 Law

The GDPR in the EU and the 2017 Law in Guernsey are game-changers, a fundamental shift towards an accountable model of digital society.

First, many of the principles in the earlier legislation remained valid and were carried over, with some improvements.

For example, the definition of **personal data**[1], which remains very broad, and the principle of **purpose limitation** (personal data must be collected for specified, explicit and legitimate purposes) were preserved.

[1] Any information relating to an identified, or identifiable, individual.

The notion of consent has been reinforced to make it stronger: consent may be withdrawn at any time, and it should be as easy to withdraw consent as to give it.
Finally **the right to erasure, to be forgotten**, **is reinforced**. Individuals can ask that a link be delisted from a search engine or data be deleted if they violate their privacy. Individuals can simply withdraw their consent or object.

The new legislation also contains a number of significant innovations designed to respond to the new technological and commercial challenges. For example, the right to **data portability** gives individuals the power to change which service provider or social network handles their personal information.

Where there is **profiling and automated decision-making**, individuals must be specifically informed about the existence of such decisions and their envisaged consequences for the individual, and their consent must be obtained where the profiling has a legal or significant effect, e.g. decisions on credit worthiness.

More generally, one of the main innovations of the GDPR is that it is a '**Regulation'**, which applies directly at national level in every EU Member State, like a Law adopted by the States of Deliberation.

The existence of a single overarching set of rules across the EU provides a harmonised legal framework for Guernsey entities to transfer data across the EU and the EEA.

Probably the main innovation in the GDPR and in the 2017 Law is the **principle of accountability.** The new legislation makes companies and public authorities accountable for their data practices in a very specific way.

Every data controller must do three things:

1. include data protection in **advance** in the planning and design of new data processing and **implement** the appropriate technical and organisational measures;
2. ensure that these measures are in **compliance**;
3. and be ready to **demonstrate** that it has taken the steps needed to comply.

There is no threshold on this obligation, but it is scaleable, according to the nature of the organisation processing personal information and on the level of risk for the individuals concerned.

It is worth mentioning that the ODPA has planned a special conference for small and medium size organisations, in 2021, to discuss what accountability means for them in practice.

In a nutshell, accountability means *actively developing compliance and being able to demonstrate such compliance*. So an accountable organisation will do the following:

- appoint and support expert data protection professionals
- ensure top management commitment
- map its data processing activities and use data protection impact assessments where appropriate
- adopt and implement the necessary policies and processes
- make these policies transparent - for data subjects, regulators and the general public
- implement systems for internal ongoing oversight, and
- install mechanisms for remediation and external enforcement.

And it is worth investing in being accountable. For example, an accountable company which respects its data security obligations will have taken precautions against personal data breaches. And then, if there is a data breach, it will have the procedures in place to identify and to notify the breach. This will both reduce the harm to data subjects and reduce the level of exposure of the controller to sanctions and loss of reputation.

Finally, **the GDPR strengthens enforcement.**

For the first time, the GDPR and the local 2017 Law empower data protection authorities to impose rigorous **administrative and financial sanctions** - up to €20m or 4% of worldwide turnover of the preceding year, whichever is the greater, under the GDPR, and up to £300,000, or 10% of the total global annual turnover or total global gross income of the preceding year, whichever is the greater, under the local 2017 Law.

This new element of dissuasive sanctions is a crucial part of modern data protection law, it provides competition law-style sanctions for breach, and makes data protection a key issue for top management.

However, fines are only a means to an end.
Most organisations prefer to respect the rules, so far as they can know and understand them.

The GDPR and the 2017 Law marked the beginning of a learning process, both for organisations and for the individuals whose data they process.

In the Bailiwick, the ODPA *Strategic Plan (2019-2022)* stresses the positive approach of the Authority to assist and advise the regulated community, and the Plan was recently updated to permit constructive exploration of innovative practices and activities by controllers.

The success of the GDPR and the local 2017 Law will be measured, not in the number of fines imposed, but rather in changes in the **culture and behaviour** of everyone involved.

When organisations 'do the right thing' with our personal information, treat it with the care and respect it deserves, and honour our rights over how it is used, we will have succeeded.

Excellence Through Ethics.

+44 (0) 1481 742074 | enquiries@odpa.gg | odpa.gg