Association Network

GENERAL DATA PROTECTION REGULATION (GDPR)

Professional Guidance: IT 2
Original Publication Date: December 2018©

INTRODUCTION

GDPR will not fundamentally change data or how we choose to use data. However, it will make organisations take a closer look at why they keep data, how it is used and the length of time information is retained. Indeed, the burden of ensuring compliance will shift considerably towards the organisation holding data and it will be up to them to prove that they have the clear legal basis to justify processing the data.

GDPR is aimed at creating a culture where it is appreciated that data has value, and that there is a right to privacy and accountability for data and its use. It is not expected that all users of other people's data become legal experts overnight, rather that organisations are seen to be developing and evolving policies to ensure that measures have been taken to minimise risks of breaches and misuse, thereby respecting the rights of those whose data is held by third parties. Organisations should not just be responsible for information they hold, but also be able to demonstrate compliance that these obligations are being met, and rights have been respected. In practice this means additional paperwork confirming a clear lawful basis to use data, whether by your organisation or by third parties. Establishing whether your organisation is a Data Controller or a Data Processor for the different personal data you process is key.

OVERVIEW

Although 25th May was designated the day for the introduction of the Regulation, this was clearly not a deadline. The Regulation will come into force and develop and evolve and it remains to be seen how the courts will interpret it. However, there are certain fundamentals which will need to be respected:

- What are the details of the data being held?
- Why is the data being held?
- What are the rights of the data subject?
- How long has it been kept and under which circumstances should the data be deleted?
- What constitutes consent?
- What is the basis for keeping the data? Can you rely on consent, or "Legitimate Interests" or is there a contract in place?

The Regulation will also look at issues of confidentiality and "control". For example if a laptop computer containing highly sensitive information is stolen from a car boot which has been locked, has there been deemed to have been sufficient exercise of control over the person from whom it was stolen and the procedure for transport of such sensitive information? In practice, the Regulation will take a view on the role of those involved and whether there had been sufficient clarity in procedure and whether this had been properly documented.

GENERAL DATA PROTECTION REGULATION (GDPR)

Professional Guidance: IT 2
Original Publication Date: December 2018©

The ICO will not be employing larger numbers of auditors. However, there is an increasing expectation that organisations which suffer serious breaches will need to engage much more closely and quickly with the ICO. It is not only a matter of financial loss and loss of privacy but also damage to Trust, Brand and Reputation which organisations face. Individuals will have increased rights which opens the doors for "ambulance chasing lawyers", so to protect themselves organisations will have to demonstrate that they have taken reasonable steps and that actions have been proportionate.

HOW WILL THE REGULATION BE ENFORCED IN PRACTICE?

Prohibition of use of data without clear justification.
In particular, the use of sensitive information (special category personal data) is prohibited unless a clear justification defined in the legislation can be found to justify the processing.

Where consent is required to process data, clear records of consent must be held. A lack of response is not regarded as a tacit way of granting consent. Furthermore, different consents are required for different types of processing – if the individual should have choice, then obtaining one "overall" consent will not be sufficient.

Where legitimate interests are used to justify processing data, a balancing exercise is needed. The concept is an attempt to balance the needs of the Association or affiliate with the interests of the individual as data subject, such that it does not "override" the fundamental rights and freedoms of the data subject.

The purpose behind why you are processing data provides guidance as to how long should data be kept. The data controller has the ultimate responsibility for managing the information and defining who should keep the data and for how long.

This may be uncomfortable for associations especially if some services are contracted out but the whole point about GDPR is that there is clarity over procedure and lines of accountability.

Process.
There is no legal requirement to do this precisely but a suggested means of process could be:

- Foundation
  - availability of records if required
  - management of key GDPR requirements, such as a policy framework
  - clear records of processing activity
- Intermediate
  - documentation of data journeys
  - evidence of a privacy information strategy
  - relationships between those holding the data and the data subjects
  - information security – are adequate controls in place?

GENERAL DATA PROTECTION REGULATION (GDPR)

Professional Guidance: IT 2
Original Publication Date: December 2018©

The law will be subject to interpretation but the current discussion takes the view that if the Data Controller has a contract with an outsourcing organisation "the data processor" then the Data Controller will have responsibility for the management of that data, even though in many cases they might not even see large amounts of this data.

It is critical that all parties understand their respective expectations. Organisations should exercise:

- due diligence during the course of their work
- contractual control over those working for them and for their clients
- monitoring and appropriate supervision over their affiliate counsellors

Affiliates are often involved in remote working and should take account of the need for:

- information security
- secure storage of information
- consistent handling of information and record retention
- appropriate record disposal in line with expectations

Data Subjects.
Associations need to be clear about what they are managing and how to meet expectations. What is crucial is that they need to be clear about the purpose of their processing activities, how the data is stored and how it is used/shared. This determines how much data they can collect and who needs to see it, and how long they can hold it for. The Data Subject has the right to request access to information held by Data Controller, and on their behalf by third parties.

ACCOUNTABILITY

This defines:

Readiness Assessment

- process should define that a data breach should be reported within 72 hours
- Data Subjects should have access to data without charge for 30 days following a data breach
- Data Controllers should be able to defend any proposed reliance on "Legitimate Interests" to process data
- Data Subjects can withdraw their consent at any time and have right to erasure.

Transparency
The obligations around transparency are intended to be “user centric” rather than “legalistic” so people can easily understand what is happening to their data, why, and what rights they have.

This is outlined in Articles 12-14 and requires privacy information to be:

- detailed and specific
- easy to assimilate and be accessible
- part of a good set of channels of communication
- part of good record keeping

Security.
Where possible this should:

- be the State of the Art so as to minimise breaches and hacking
- based on the nature, scope, context, and purpose of processing
- reflect the risks and varying likelihood of breaches
- respect the rights and freedoms of data subjects.

An appropriate technical and organisational framework should be in place.

CONCLUDING REMARKS

- Organisations have a duty of care over client confidentiality
- Organisations provide services to members and however they are to be delivered as defined by a contract does not detract from the fact that the Employer is the Data Controller.
- "Legitimate Interests" cannot be used for special categories of personal data (sensitive personal data).

In short, the advent of the Regulation heralds an era of expectations of tougher controls and the possibility of greater fines. But in practice, what it aims to engender is a greater sense of the value of data being held, greater responsibility of the organisation holding it, and an understanding of the increased rights of Data Subjects. The focus and direction of implementation will depend on the results of cases in the courts which will create precedent.