Policy Briefing

Chartered Insurance Institute
Standards. Professionalism. Trust.

23 October 2017

General Data Protection Regulation: issues and challenges

Key Points:

- The General Data Protection Regulation (GDPR) comes into force in May 2018 replacing the existing Data Protection Act.
- It recognizes that the protection of individuals in relation to processing personal data is a fundamental right.
- The GDPR sets a high standard for consent. Consent means offering people genuine choice and control over their personal data is used.
- The GDPR applies to all persons who control and/or process personal data. The regulation distinguishes and has specific obligations for "controllers" (those who say how and why personal data is processed) and "processors" (those who act on the controller's behalf).

What is the GDPR?

The European General Data Protection Regulation (GDPR) will from May 2018 underpin all data protection standards, and replaces existing laws and regulations. It will apply to all organisations (wherever they are) that are holding personal data on individuals in the EU including the UK.[1]

Scope

Its application includes firms (wherever they are) that are offering goods or services or monitoring the behavior of individuals in the EU:

- Offering goods and services (irrespective of whether payment is required): more than mere access to a website or email address, but might be evidenced by use of language or currency generally used in one or more member states
- Monitoring behavior: includes tracking on the internet by techniques applying to a decision profile

The GDPR applies to all persons who control and/or process personal data. The regulation distinguishes and has specific obligations for "controllers" (those who say how and why personal data is processed) and "processors" (those who act on the controller's behalf).

Oversight

Like the Data Protection Act (DPA) it replaces, GDPR will be overseen in the UK by the Information Commissioner's Office.

Financial services firms should note that the Financial Conduct Authority (FCA) could also be involved in particular cases involving financial services firms, because data protection law breaches also highlight concerns about a firm's overall systems and controls.

Application

GDPR goes further than the DPA in that it widens the application of "personal data". For example it includes online identifiers such as IP addresses constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most firms doing tasks like keeping HR records, customer lists, or contact details, the change to the definition should make little practical difference. Many have complied for years.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Data processing rights to individuals

The GDPR creates some new individual right and strengthens some rights currently under the DPA.

The right to be informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data. The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The right to give and withdraw consent

Allied to the right to be informed is the high standard for consent. Consent means offering people genuine choice and control over how their personal data is used.

The GDPR definition of consent is: *"…any freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her."*

[1] The Government has confirmed that Brexit will not affect the commencement of GPDR, but it is possible that questions might arise at a later stage stemming from the negotiations.

This means no pre-ticked boxes but clear affirmative action agreeing to the processing of personal data.

The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Personal data processing principles

Personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing such as for archiving purposes in the public interest is considered compatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest (re 2 above);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These are similar to existing DPA subject access rights. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing

The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If personal data in question is disclosed to third parties, the discloser must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

The right to erasure

The broad principle is to enable one to request deletion or removal of personal data if there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent. Withdrawing consent must be as easy as giving consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);
- The personal data has to be erased in order to comply with a legal obligation; or
- The personal data is processed in relation to the offer of information society services to a child.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

The right to restrict processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

- Services cannot be made conditional on consent for unrelated processing; and
- Each purpose of processing requires separate, specific consent.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling.

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.