FYI®
For Your Information®
UK

Volume 2017 | Issue 49 | 20 July 2017

Preparing for the General Data Protection Regulation

The European General Data Protection Regulation (GDPR) will have direct effect in all European Union Member States from 25 May 2018 and will replace the Data Protection Act 1998 (DPA). It will also apply to organisations outside the EU that process personal data in relation to individuals within the EU and will impact on the UK post-Brexit.

Whilst the GDPR has been described in some quarters as 'evolution, rather than revolution', it represents a raising of the bar for both data controllers (such as employers, pension scheme trustees and scheme actuaries) and data processors (e.g. pensions administrators, payroll providers and insurance companies).

Introduction

The DPA has been in force for nearly 20 years and organisations complying properly with the current law will be aware of the principles. There are, however, some significant enhancements and new elements under the GDPR (such as the need to demonstrate accountability) and preparation for compliance with the GDPR is expected to take some time to implement as there is substantial work to do to document and comply under the new procedures.

Guidance from the Information Commissioner's Office (ICO)

In the UK the supervisory authority responsible for data protection is the Information Commissioner and it produces guidance to help organisations prepare and comply. In its published checklist, the ICO highlights 12 steps, starting with ensuring decision makers in the organisation are aware of the GDPR, and including the documenting of policies and procedures, revised privacy notices, through to the complex arrangements that apply where an organisation operates internationally – a common situation in a global society.

The intention of this briefing note is to highlight some of these steps so that organisations (data controllers) such as pension scheme trustees and employers, as well as service providers (data processors) can start to prepare for May 2018.

Definitions

A quick look at the various definitions used in the GDPR will be useful in refreshing current knowledge of the data protection principles and how these have been expanded in the GDPR.

Controller

The controller determines the purposes and means of the processing of personal data (i.e. how and why personal data is processed). A controller remains responsible even where a processor is involved and the GDPR places further obligations on the controller to ensure contracts with processors comply with the GDPR.

Processor

The processor processes personal data on behalf of the controller. The GDPR places specific legal obligations on the processor (e.g. a processor is required to maintain records of personal data and processing activities). A new requirement means that a processor has legal liability if it is responsible for a breach and will mean that processors will need to notify controllers of any security breaches.

Personal data

This is any information relating to an identified or identifiable person (i.e. a person who can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The definition is more expansive than that under the DPA, reflecting changes in technology (e.g. an IP address is deemed to be personal data).

Special categories of personal data

This replaces the current definition of sensitive personal data, but is essentially the same. It would include:

- personal data that reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership,
- genetic data (inherited or acquired genetic characteristics),
- biometric data (specific technical processing relating to physical, physiological or behavioural characteristics),
- data concerning a person's physical or mental health (including the provision of health care services, which reveal information about health status),
- data concerning a person's sex life or sexual orientation.

Processing

This includes collection, recording, organisation, structuring, storage, retrieval, erasure or destruction amongst other actions, whether or not automated.

Filing system

This includes any structured set of personal data whether centralised, decentralised or dispersed on a functional or geographical basis. The GDPR is wider than the DPA and could include chronologically ordered sets of manual records containing personal data.

Accountability

The data protection principles are similar to those in the DPA but the most significant addition is the accountability principle. The GDPR requires organisations to show how they comply with the principles – for example by documenting the decisions taken about a processing activity. The GDPR states explicitly that this is the responsibility of an organisation and the ICO guidance lists governance measures such as:

- staff training, internal audits of processing activities and reviews of internal HR policies,
- maintenance of relevant documentation on processing activities.

Actions

Awareness

Advise decision makers and key people of the changes in the law, so that they can appreciate the impact these are likely to have and identify areas that could cause compliance problems. An organisation's risk register is a good starting point.

Identification of data

Arrange an information audit to document what personal data is held, where it came from and who it's shared with. The GDPR, for example, requires organisations to let another organisation know where it's established that personal data that has been shared with another organisation is inaccurate so that it can correct its own records too.

Privacy (fair processing) notices

Review current privacy notices and get ready to make any necessary changes. A privacy notice lets people know who is holding their personal data and how the information is to be used. The GDPR requires organisations to explain the legal basis for processing the data (see below – if the legal basis is for the controller's legitimate interests, this needs to be explained), the data retention period and the right of an individual to complain to the ICO if they think there is a problem with the way their data is handled.

Individuals' rights

Check procedures to ensure they cover all the rights individuals have, including how personal data will be deleted or provided electronically in a commonly used format.

Subject access requests

Update procedures for handling requests for copies of personal data. Under the GDPR an individual cannot be charged for asking to access copies of personal data and normally this must be supplied within a month rather than the current 40 days. Additional information will also need to be supplied to the individual, such as the data retention period and the right to have inaccurate data corrected.

Legal basis for processing personal data

Identify and document the legal basis for processing data. Under the GDPR some individuals' rights will be modified depending on the legal basis for processing their personal data. For example, where consent is the legal basis, an individual has a stronger right to have their data deleted. This legal basis will have to be explained in a privacy notice and when a subject access request is answered. Organisations should take legal advice on the appropriate basis for processing data.

Alternative bases include:

- performance of a contract to which the person is a party,
- compliance with a legal obligation to which the controller is subject,
- to protect the vital interests of the person,
- for the controller's (or a third party's – such as the processor's) legitimate interests.

Consent

Review how consent is sought, obtained and recorded, and whether this remains the most appropriate legal basis (as above). Under the GDPR both consent (including explicit consent) need to be freely given, specific, informed and unambiguous. It needs some form of clear affirmative action. Silence, pre-ticked boxes or inactivity no longer constitute consent. It also needs to be verifiable and an individual has the right to withdraw consent at any time.

Children

Consider whether parental or guardian consent is required for processing personal data of children (under age 16 although EU Member States can reduce this to age 13). This is more likely to impact social networking service providers.

Data breaches

Review procedures for detecting, reporting and investigating a personal data breach. The GDPR requires organisations to report breaches (within 72 hours) where the individual is likely to suffer some form of damage (such as identity theft or a confidentiality breach) and notify the individual whose data has been breached (e.g. where it might leave them open to financial loss). Failure to report a breach when required could result in a fine as well as a fine for the breach itself.

The maximum fines under the GDPR are 20 million euros for serious breaches (or 4% of annual worldwide turnover for commercial entities if higher) and 10 million euros for breaches of lesser provisions (or 2% of annual worldwide turnover if higher).

Data Protection Impact Assessments

Consider the requirements for these assessments, for instance, where a new technology is being deployed and this is a high-risk situation. A Data Protection Impact Assessment is an assessment of the impact of the processing operations on the protection of personal data and allows an organisation to identify and fix problems at an early stage.

Data Protection Officers

Consider whether a Data Protection Officer needs to be appointed. This is more likely to impact public authorities whose activities involve the regular and systematic monitoring of people on a large scale. The GDPR requires that a Data Protection Officer has professional experience and knowledge of data protection law.

International

Consider mapping out where in the world significant decisions about data processing take place. Understand the restrictions imposed by the GDPR on the transfer of personal data outside the European Union. Adequate safeguards must be provided.

Conduent HR Services

A working party has been established to consider the impact of the GDPR on Conduent HR Services in our role as controllers and processers of personal data on behalf of our clients. We are actively preparing for the new legislation by taking the actions, as appropriate, set out above. We are also reviewing and updating our contracts with clients and other third parties to ensure that we are compliant by 25 May 2018. Your consultant will be in touch to discuss this in due course.

Authors
Nikki Williams, Senior Technical Consultant
John Dunkley, Senior Technical Consultant
Gary Crockford, Technical Services Manager

Produced by the Knowledge Resource Centre
The Knowledge Resource Centre is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your consultant or call us on 0800 066 5433.

CONDUENT