STEP UK Briefing Note: General Data Protection Regulation (GDPR)

Published 5 March 2018
Updated 9 January 2019

INTRODUCTION

Since 25 May 2018, UK organisations processing personal data have been required to comply with the EU *General Data Protection Regulation* (GDPR). As a STEP member, you were already required to comply with the *Data Protection Act 1998* (DPA) prior to the GDPR.

Although the GDPR will cease to apply directly in the UK once we leave the EU on 30 March 2019, the *Data Protection Act 2018* (DPA 2018) effectively incorporates an equivalent set of rules into the UK's domestic law and so the new regime should be considered to be 'Brexit-proof'.

In the UK, the accountancy and legal regulatory bodies have developed resources to enable those they regulate to prepare for and implement the changes required under the GDPR, and we encourage our members who are regulated with those bodies to use the tools available.

This briefing note is not intended to provide our members with legal advice on the changes to data protection in the UK; nor does it set out all the activities that you are required to undertake to ensure that you are GDPR-complaint. You should always take professional advice when appropriate.

The aim of this note is to provide you with an overview of the legislation, highlight the core changes to UK data protection law made by the GDPR and give some general assistance on what you can do to ensure you are compliant. For the avoidance of doubt, you are required to comply with any existing professional regulations. The GDPR does not replace any other rules, it simply enhances data protection.

WHAT IS THE GDPR?

Essentially, the GDPR is a set of data protection requirements laid down by the EU. The GDPR's main principles and concepts are generally similar to those that applied under the UK's previous DPA, but there are significant differences to be aware of.

The UK government has used the DPA 2018 to incorporate the GDPR into its existing data protection framework.

In addition to data controllers, the GDPR also applies directly to data processors. By way of reminder, a 'data controller' is a person or entity who determines how and why personal data will be processed, whereas a 'data processor' is a person or entity responsible for processing personal data on behalf of a data controller.

We anticipate that most accountancy and legal practices will be data controllers for the purposes of the legislation.

The GDPR has a wide territorial scope and applies to data controllers and data processors who:

- operate within the EU; or
- operate outside the EU, where their activities relate to EU individuals.

HOW SHOULD YOU ENSURE THAT YOU ARE COMPLIANT WITH THE GDPR?

Most organisations that were compliant with the previous DPA will not have faced a significant challenge in terms of complying with the GDPR. However, they will have noticed changes and additions to their legal requirements.

Notably, obligations on data controllers and data processors are increased, and the rights of individual data subjects are strengthened. The GDPR also includes a new principle of 'accountability' under which organisations must be able to demonstrate compliance with the rules. In other words, they must proactively consider their position under the GDPR and maintain records to evidence their compliance, as opposed to retrospectively justifying processing personal data as and when they are challenged.

Other core changes:

- Data controllers are responsible for ensuring compliance by those to whom they subcontract data processing ('data processors').
- Data processors are, in addition, more directly responsible for their own data processing activities.
- You should consider carrying out data protection privacy impact assessments where appropriate, which will enable you to assess risk and ensure you have developed effective and efficient processes for handling data.
- Individuals have enhanced rights regarding the data you hold on them, including the right to certain specific information, the right to object to certain processing, the 'right be forgotten', a right of access to their data, a right to data portability etc.
- All data processing must be based on one of several legal justifications in the GDPR (and the processing of special categories of personal data is only permitted if one of a limited set of exemptions applies).
- Consent should no longer be the default option for justifying data processing and may not be applicable in many cases owing to increased requirements (see below).
- In certain circumstances, breaches of data security must be reported to the Information Commissioner's Office (ICO) within 72 hours, and there is an obligation to notify individuals of breaches that pose a high risk to their rights and freedoms.
- In addition to the risk of reputational damage resulting from a data breach, there are increased financial penalties. These can be up to EUR20 million or 4 per cent of your global turnover (whichever is higher). There is also the potential for damages where an individual suffers loss as a result of a data breach.

it is unlikely that small organisations will require a data protection officer unless personal data is being processed on a large scale but you should consider whether it is sensible to appoint one anyway, or whether you should create a similar role such as a 'data protection administrator'.

The ICO has provided an online tool to assist organisations with determining whether they need a data protection officer. The tool is available at https://ico.org.uk/for-organisations/does-my-organisation-need-a-data-protection-officer-dpo/

Before the GDPR was introduced, the ICO also produced a guide on how organisations should prepare for the GDPR. This can still be a helpful reference point when considering whether your organisation is now compliant and the 12 steps that it suggested are set out below.

(1) Raise awareness

Key decision makers have overall responsibility for implementing GDPR and must be aware of the changes required and plan for any resource implications.

(2) Know what information you hold

- Document all the personal data you hold on individuals, including:
    - how you obtained the personal data; and
    - with whom you share the personal data.
- Carry out an internal audit of all your data-processing activities.
- Review/revise your policies and procedures for all your data-processing activities.
- Develop policies and procedures if they are not already written down.

(3) Communicate your privacy information

The GDPR generally requires you to inform individuals whose data you process of the following:

- The contact details of your data controller.
- Why you are processing an individual's data.
- The lawful basis under which you are processing their data.
- Who receives the personal data an individual shares with you.
- Whether personal data is transferred outside the European Economic Area (EEA).
- What your data retention periods are, and that individuals have the right to complain to the ICO if they are concerned how their data has been handled.
- The existence of the individual's various data rights under the GDPR (such as the right to access their personal data).

You may also be required to provide this type of information to an individual when you receive personal data relating to them from another source.

Your privacy policy must be concise, clear and easy to understand.

(4) Communicate your privacy information

There are new rights for individuals as mentioned above. You need to make sure your systems and policies are set up to allow you to accommodate any request from a data subject.

Be clear that you know what you would do and how you would respond e.g. if an individual asked you for access to their personal data.

(5) Subject access request

A subject access request is an example of the right to access personal data being exercised. You should now process these within one month, and you can no longer charge a fee.

There are some permitted exemptions to requests for information, but you must explain why you are refusing to provide information and advise the individual that they can complain to the ICO.

(6) Lawful basis for processing data

Review your processing activities (which includes simply collecting and/or storing data) and be clear what the lawful basis is in each case. This information must be included in your privacy notice. Note that special categories of personal data (such as information relating to a person's health or sexual orientation) have even greater protection and can only be processed in a limited range of circumstances.

(7) Consent

The rules around consent have been tightened up – see the advice below on obtaining, recording and obtaining consent.

(8) Children

In most cases, data relating to children under the age of 16 should not be processed without parental/guardian consent. You should check to see whether this will affect you.

(9) Date breaches

You will need to report a data breach to the ICO within 72 hours of identifying it, if it is likely to result in a risk of an individual being affected by discrimination, reputational damage, loss (financial or confidentiality), or other potential economic or social disadvantage. You may also need to notify the individual affected if the risk is particularly high. A failure to report a breach could lead to an additional fine.

(10) 'Data protection by design and by default' and data protection impact assessments (DPIAs)

The concept of 'data protection by design and by default' requires organisations to think carefully about the processing activities they undertake, and ensure that individuals' privacy and data protection requirements are core considerations before undertaking a new project or policy development. DPIAs may help you assess and establish compliance in this area and the ICO has produced detailed guidance on this.

(10) Data protection officer(s)

A data protection officer is an individual in an organisation who is responsible for complying with data protection law. Full details of this role are laid down by the GDPR and you should check whether your organisation is required to employ a Data Protection Officer, or whether a lesser role may be appropriate.

(12) International

If your organisation operates in more than one EU Member State, you must designate a 'lead data protection supervisory authority'. This is likely to be the location of your head office. Transfer of data outside the EU will require additional consideration.

WHAT ARE THE CHANGES RELATING TO CONSENT?

There are enhanced requirements on both the controller and the processor when obtaining consent.

Consent must be freely given, specific, informed and unambiguous. The GDPR does not allow you to use a pre-ticked box to obtain consent; nor are you able to infer or assume consent from silence or a lack of response.

ICO guidance states that consent must be clear and, in order for it to be meaningful, it must not be mixed in with any other business terms and conditions. Consent requirements must be clear, concise, and expressed in language that the user can understand. We advise using plain English.

Individuals must also be advised that they have the right to amend or withdraw their consent at any time.

If consent is used to justify the processing of special categories of personal data then the requirements are even more specific.

The ICO has produced useful checklists to help you review the consent you obtain, record and manage. These are available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

RESOURCES

The ICO has developed a number of resources to help you prepare for and implement the GDPR, including written guidance, template documents, checklists, blogs and webinars, and we urge all members to review these which are available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

GDPR checklists for data controllers and data processors are available at https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/.

The ICO is regularly adding guidance on the application of the GDPR, and we advise you to check its website frequently.

ISSUES ARISING FROM IMPLEMENTING THE GDPR

The GDPR was not drafted with the world of trusts and estates in mind, and there are various ambiguities as to how it should be implemented in this context.

The STEP Data Protection Working Group is currently liaising with the ICO and other industry bodies to obtain clarification where possible. We ask that members who come across technical or practical difficulties when seeking to implement the GDPR contact us via **standards@step.org** so that the working group can take such issues into account.