Introduction

The General Data Protection Regulations (GDPR) replaces the existing Data Protection Act from 25 May 2018. The new legislation gives individuals new powers and not complying can result in fines up to 2% of an organisation's annual income. If you suffer a data breach these fines can increase to 4%. With large punitive consequences, it is important that organisations grapple with the changes at the soonest opportunity.

What are the changes?

1. **Consent:** Organisations will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. It will need to be as easy to withdraw consent as it is to give it.

2. **Breach notifications:** Notification to the regulator will become mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". Breaches will need to be made within 72 hours of having first become aware of the breach.

3. **Rights to access**: Under the new rules, individuals have the right to be informed whether personal information is being held, any processes using that information, and the purpose(s) for it being held. Furthermore, organisations are required to provide copies of all information held – free of charge if requested.

4. **Rights to be forgotten:** Also known as a "data erase", an individual can request that all data held on them is erased. This also applies to 3rd parties who are processing data on behalf of your organisation.

5. **Privacy by design**: Privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

6. **Data portability:** Individuals will have the right to receive their personal data concerning them, which they have previously provided in a '*commonly used and machine readable format*' and have the right to transmit that data to another controller.

Although these changes may at first seem innocuous, in practice there may be real challenges in implementing them. For instance, it is possible that information on individuals may have inadvertently been proliferated within an organisation.

Where I.T. restrictions have up to now been relaxed, it is possible that personal information could have inadvertently been copied to a laptop or a memory stick and if this is not controlled or understood – this poses an enormous risk to your organisation.

The standard also relates to printed material, which further increases the risk of information existing within an organisation without proper understanding of where it is stored and how it is controlled. All individuals will need to be made aware of the issues, and take responsibility for the information they hold and process.

Ensuring that all staff are clear on the importance of reporting a potential breach is also likely to require a significant cultural shift within your organisation. All of this needs to be considered well before May 2018.

What should I be doing now?

The Information Commissioner's Office has provided some helpful guidance on the steps you should be taking. We have summarised some of these points below:

1. **Raise Awareness**. Without a doubt – GDPR is going to represent a change in the way people work and deal with individual's data. Changing an organisation's culture is notoriously slow and difficult, so it is helpful to start sending out the message to all staff about the changes well before the May 2018 start date.

2. **Record your systems for holding and processing data on individuals**: This is potentially a large exercise, but it is essential that you map out how information is held within an organisation**.** This includes trying to understand what information may not be adequately controlled since it is held in unofficial repositories (such as on memory sticks, laptops or print outs).

3. **Establishing the lawful basis for processing data:** It may be that your organisation holds marketing information purchased from 3rd parties, for which you have no evidence that consent was acquired in a matter compliant with the new rules. It may be necessary to delete information where the source and consent cannot easily be established as you may, inadvertently be holding it illegally.

4. **Communicating privacy information:** The new guidelines state that privacy notices should be concise, transparent, intelligible and easily accessible. That means that the notice needs to be written in clear and plain language (and not embedded within a long list of terms and conditions).

5. **Consent to use data** will also need to be considered to ensure that it is sought, recorded and managed appropriately. It will be necessary to refresh existing consents if they do not meet the current standard. Consent can also no longer be passive (i.e. the individual needs to opt in to having their information used rather than opting out).

6. **Implementing individual's rights:** For instance, your organisation should have a plan on how it would handle a request for personal data to be erased. Anecdotally, we have heard of some IT systems which do not allow personal data to be deleted easily. If software providers are unable to bring their systems in to a compliant state before May 2018, there could be potential risks for your organisation to mitigate. Understanding the potential problems at the earliest opportunity will be important.

7. **Consider appointing a Data Protection Officer:** This individual's role is to assess whether you are complying with the regulations and to take responsibility to report a breach if there is one. It is advised that the individual should therefore sit outside the existing governance / management structure so that they are independent enough to make that assessment.

8. **Put in processes on how a data breach would be handled:** You will need to have very clear process to ensure that a data breach is detected, reported and investigated promptly. Remember, you only have 72 hours after a breach is discovered to make a report, so provisions need to be made for periods where key individuals are away from the office as well as ensuring all staff are aware of their responsibilities.

9. **Data Protection by Design and Data Protection Impact Assessments:** Data protection by design, is an approach to projects that promotes privacy and data protection compliance from the start. If your organisation is undertaking a new project involving personal data, it is important to be able to demonstrate this has been considered from the very beginning. A Data protection impact assessment will be legally required in certain situations, especially where new technology is being deployed, where any form of automated profiling of personal data takes place (such as analysis of people's interests or behaviours), or where there is processing on a large scale.

Some organisations will be seeking for external help with this transition, however, with such a short time frame before implementation, it is likely that there will be a shortage of expertise to support everyone who needs it. We think it is likely that most organisations will therefore need to tackle these risks independently.

Setting up a working group and considering the above points is a good first step, as is appointing a Data Protection Officer. However, it is important not to underestimate the amount of work that might be needed and beginning the process as soon as possible.

If you have questions or concerns please feel free to raise these with your normal contact at the firm.

Further reading

- 12 Steps to take now – published by the Information Commissioner's Office https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- General background on the new legislation published by the Institute of Chartered Accountants for England and Wales