General Data Protection Regulation (GDPR)

What is the GDPR?

The European Union (EU) GDPR was approved by the EU Parliament on 14 April 2016 and will apply to all EU countries. GDPR replaces the United Kingdom (UK) Data Protection Directive 95/46/EC and was created to bring all data privacy laws across Europe into harmony. In the UK the Information Commissioner's Office (ICO) is an independent authority which upholds the UK legislation relating to Data Protection and other public information rights.

GDPR is relevant to every organisation, no matter how large or small, who collect 'personal data' about EU citizens. The GDPR also regulates the exportation of personal data outside of the EU, for example, the storage of personal data on a server based outside of the EU.

GDPR defines several roles:

- The data controller. The data controller defines how personal data is processed and the purposes for which it is processed; and
- The data processor. The processor may be an internal group who maintains and processes personal data, or it may be an outsourcing firm that performs those activities.

Under GDPR both the data controller and the data processor can be held responsible for breaches or non-compliance with the legislation.

When does GDPR apply?

The ICO have advised that GDPR will apply in the UK from 25 May 2018, as part of EU law and it is planned that, following the UK's exit from the EU the law will be enshrined in UK statute in the Data Protection Bill which is currently going through Parliament.

What is the difference between GDPR and the Data Protection Act (DPA)?

It is important to note that many of the core requirements and principles of the DPA will be subsumed into GDPR. These requirements include fairness, lawfulness and transparency, purpose limitation, data minimisation, accuracy, storage minimisation, security, integrity and confidentiality. However, the GDPR will require demonstration of how it is implemented and how compliance with the legislation is being achieved.

As current data protection law was written more than 20 years ago, before the digital information age, the GDPR has expanded to cover these areas, including (but not limited to) an expansion of what is considered 'personal data', the 'right to be forgotten' and right the 'data portability'.

What is ‘personal data’ under GDPR?

Under GDPR personal data is defined as any information relating to an identified or identifiable natural person (also known as a data subject), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

Personal data identifiers can include basic identity information e.g. name, address, email addresses, date of birth, ID numbers, web data such as location, IP address, Cookie tags. The GDPR applies to both automated personal data and to manual filing systems.

Some categories of data are classified as ‘sensitive personal data’ and require more rigorous grounds for processing. Sensitive personal data includes (but is not limited to) racial or ethnic origin, political opinions, religious beliefs and have also been expanded to include genetic and biometric data.

What personal data am I allowed to process?

The grounds for processing personal data broadly replicate those under the DPA, therefore many organisations will just need to review and update their existing Data Protection policies. The processing of personal data is legal under the following conditions:

- Consent of the data subject. Under GDPR consent must be explicit and a positive opt-in. Additionally it must be specific to the purpose. For example, you cannot gain consent for one aspect of business and then assume consent for an entirely different aspect of your business;
- Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract;
- Necessary for compliance with a legal obligation;
- Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent;
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. These functions must arise under Member State or EU law; and
- Necessary for the purposes of legitimate interests – this condition can no longer be relied on by public authorities.

There are more stringent grounds for processing ‘sensitive data’, however these remain broadly similar to the DPA grounds for processing sensitive data.

What are the implications of not being compliant with GDPR

The potential fines for breaches under GDPR (a maximum of £17 million or 4 per cent of turnover depending on the breach) are far greater than under the DPA (a maximum limit of £500,000). However, in August 2017 the ICO published a blog article called **‘sorting the fact from the fiction’** which highlighted that the ICO prefers to guide, advise and educate organisations about how to comply with the law. The ICO further explained that in 2016/2017 they concluded 17,300 data protection cases. Of which only 16 of them resulted in fines for the organisations concerned.

Next steps and further information

The GDPR is a comprehensive new law which will require individual organisations to assess how they best demonstrate compliance with their statutory requirements under the legislation.

If you haven't started to prepare for GDPR the ICO have released detailed guidance to help businesses become compliant with GDPR before the deadline of 25 May 2018.

In particular '12 steps for preparing for the GDPR' which can be found here:
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

You can also access all of the detail, definitions and guidance from the ICO at the following link:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

You can assess your organisation's readiness against the ICO's 'Getting Ready for GDPR checklist' which can be found at this link:
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

The ICO has a dedicated advice line for small organisations and charities which can be called on 0303 123 1113 (select option 4). Additionally they provide a live chat support option through the computer which allows a transcript of the conversation to be saved or printed for future reference. The ICO phone line and web live chat service can be incredibly busy with long wait times. It is best to try and call as close to 9am as possible. The service is available Monday to Friday.

The ICO also have a Frequently Asked Questions (FAQ) page for charities concerned about GDPR which can be accessed here:
https://ico.org.uk/for-organisations/charity/charities-faqs/

Furthermore, ACAS have published key points about the GDPR in relation to employees. You can read the key points here: **http://www.acas.org.uk/index.aspx?articleid=3717**