General Data Protection Regulation

1 Data protection act 1998

In 1998 the Data Protection Act 1998 came into force across the United Kingdom. This Act essentially aligned British law with the 1995 EU Data Protection Directive. The aim of the legislation was to regulate the way in which personal data is processed and it introduced a number of rules and principles that entities who process personal data must adhere to.

This legislation is primarily focused on the Data Controller and how they use the personal data of the Data Subject (an individual). Data Controllers are defined as the entity that establishes how and for what purpose the individual's personal data is processed; they are required to (and are liable for) processing data in line with eight privacy principles which state personal data shall be:

1. Processed **fairly and lawfully**;
2. Obtained for one or more **specified lawful purposes**, and not further processed in a manner incompatible with those purposes;
3. **Adequate, relevant and not excessive** in relation to the purpose;
4. **Accurate and up to date**;
5. Shall **not be kept longer than necessary** to achieve the purpose for which it was gathered;
6. Processed in accordance with the **rights of the Data Subject**;
7. **Appropriate measures and safeguards** are taken to protect personal data from unlawful loss, damage or destruction; and
8. Shall **not be transferred to a country outside the EEA** unless that country ensures an adequate level of protection for the rights of the Data Subject in relation to processing personal data.

A major criticism of the Act is that it is relatively old, having come into UK law in 1998 – since the Act's implementation there have been huge advances in technology and the way businesses use and process personal data. Similarly it was seen as a weakness that the DPA does not directly hold Data Processors (entities that process personal data on behalf of the Data Controller) liable for breaches or non-compatibility with the Act. The EU decided to address these problems, and at the same time sew together consistent legislation from the patchwork of separate data privacy legislation found across the Union.

2 GDPR

General Data Protection Regulation (GDPR) will come into force across the UK and the rest of the European Union in May 2018 and will essentially replace the 1998 Data Protection Act. Although it shares a number of common themes and principles with the DPA (access to data etc) the GDPR goes

much further, enhancing the Data Subject's rights, increasing transparency and introducing methods to better ensure compliance with the legislation.

A key difference between GDPR and the Data Protection Act is that Data Processors will also be covered by the responsibilities of the Regulation and will therefore share liability for breaches or incompatibility with the legislation. As a result it is likely that Data Controllers will only engage and work with Data Processors who are able to adhere to the Regulation. It is also likely any contract between these parties will reflect the responsibilities each party shares under this legislation.

Organisations processing personal data will be expected to be upfront and transparent in the way they process an individual's personal data, and consent will need to be both clear and unambiguous if it is to be relied upon for the processing activity. Other enhanced subject rights include the **right to be forgotten**, **right to data portability** (allowing data subjects to transfer their personal data from one data controller to another), and **right to restrict or object** to data processing activities.

The Regulation also highlights a number of technical and organisational measures which businesses/firms/entities should consider and employ, to ensure data protection is considered throughout any processing activities. These include the concept of '**Privacy by Design**' whereby processing activities are formally assessed and reviewed to ensure compliance with the Regulation and reduce any risks associated with the action.

Businesses processing personal data are also advised (or instructed in certain instances) to appoint a **Data Protection Officer** (DPO). It will be the job of the DPO to assist entities to achieve and maintain compliance with the Regulation and be involved with formulating suitable policies and controls.

Importantly, it should be noted there is a 'stick' for businesses who fail to comply with Regulation; this takes the form of hefty fines, up to **20 million Euro or 4% of the annual turnover** of the business (whichever is greater).

GDPR is largely positive as it brings consistency across the EU, giving Data Subjects confidence the same rights (including the right to remedy) will exist regardless of which EU country data is processed. It is also the case that GDPR will apply to organisations outside the European Union who process the data of EU citizens. The Regulation appears to bring much more balance to the playing field between business and the individual, in regards to how their personal data is used, and is likely to drive forward fair and transparent practice. The message is clear: compliance gives the opportunity for entities to create good business practices and develop trust through transparency with Data Subjects, however deviation from these principles will not be tolerated.

3 Further information

Vero maintain an extensive library of documents relating to screening specific topics, including legislation and regulation. If you require further information on this or any other topic, please contact your Client Relationship Manager or get in touch via the 'contact us' page on our website.