StotenGillam
chartered accountants
chartered tax advisers

Telephone: 01582 608601
Fax: 01582 667390
Email: enquiries@stotengillam.co.uk

www.stotengillam.co.uk

Data Security – General Data Protection Regulation - Ensuring Compliance

The General Data Protection Regulation (GDPR) replaced the existing Data Protection Act and applies from 25 May 2018.

The GDPR requires all organisations that deal with individuals living in an EU member state to protect the personal information belonging to those individuals and to have verified proof of such protection. Failure to comply with the regulation will result in significant fines.

Whilst there are similarities between the Data Protection Act and the GDPR, there are some new and different requirements that all businesses need to be aware of. This factsheet will help you consider whether you have carried out the steps to ensure you have adequately prepared and are compliant with the regulations.

We have also produced a related factsheet entitled 'Data Security – General Data Protection Regulation', which covers the principles behind the regulations.

Summary of new and modified requirements

Here we summarise the new/modified requirements of the GDPR in comparison to the Data Protection Act.

There are perhaps a number of overriding principles and key words within the GDPR. These include transparency, accountability, consent, compliance and privacy by design. Some of the areas where these impact include:

- **Controllers and processors** – there are some specific legal obligations for controllers and processors.
- **Controllers** – must specifically ensure that contracts with processors comply with the GDPR. Controllers shall also be responsible for, and be able to demonstrate, compliance with the GDPR data protection principles - including appropriate documentation.
- **Processors** – are required to document records of personal data and processing activities, and are also legally responsible and liable for any security breaches.
- **Privacy notices** – the GDPR promotes transparency over processing by way of a privacy notice encompassing (amongst other things) details of the controller, the source of the data, recipients of the data, data transfers made outside the EU, and the retention period of the data.
- **Consent** – consent must be freely given, specific, informed and unambiguous. Positive consent can no longer be inferred from silence, inactivity or the use of pre-ticked boxes.
- **Children's personal data and consent** – there are special provisions relating to the consent and processing of children's personal data.
- **Accountability and governance** – organisations need to have 'comprehensive but proportionate' governance measures. For many organisations this is likely to mean more policies and procedures. And, for larger organisations (over 250 employees), this also means assigning or appointing a Data Protection Officer (DPO).
- **Subject Access Request (SAR)** – the time to respond to a SAR is now 30 days, and it must be provided free of charge unless the request is unfounded or excessive.
- **Notification of breaches** – breaches must be reported within 72 hours to the relevant supervisory/ regulatory authority.
- **Data portability** – this is a new right under the GDPR, and allows an individual to request a machine readable copy of their personal data where processing is carried out by automated means.

Summary of key preparatory steps

The ICO have produced a twelve step checklist to help organisations get themselves ready for compliance.

1. **Awareness** – the decision makers and key people in the organisation need to be made aware that law is changing. They need to appreciate the impact, and quantify and allocate resources to ensure compliance.
2. **Information held** – what personal data is held, where it came from and who it is shared with should be documented. It may be necessary to arrange for an information audit to be performed.

3. **Communicating privacy information** – existing privacy notices should be reviewed, and, if necessary, updated. Enhanced disclosure may be necessary to take into account all the new rights of individuals. If a privacy notice(s) does not exist, then one will need to be constructed.
4. **Individuals' rights** – review the eight key rights individuals have under the GDPR, and whether existing procedures and policies cover all these rights.
5. **Subject access requests** – update subject access rights procedures to take into account the rules.
6. **Lawful basis for processing personal data** – the lawful basis for processing activity should be documented and communicated in the privacy notice(s) – also see three above.
7. **Consent** – consent under the GDPR relies on a positive and transparent opt-in. Existing consent mechanisms and procedures may need to be updated.
8. **Children** – children's consent and children's personal data is given special protection under the GDPR. In some cases, a parent or guardian may be required to give consent.
9. **Breaches** – the right procedures need to be in place to detect, report and investigate a breach of personal data security. All organisations must report breaches to the ICO (as well as, perhaps, their own regulatory body).
10. **Privacy by design** – this is a legal requirement of the GDPR. In particular, an Impact Assessment should be performed even where it is not mandatory.
11. **Data Protection Officer** – someone in the organisation should be designated the responsibility for compliance. A Data Protection Officer is formally required in certain circumstances.
12. **International** – if the organisation operates in more than one EU member state, a lead data protection supervisory authority needs to be nominated. This is usually the country in which significant decisions are made about processing activities.

Documentation

Documentation of the processing activities carried out by the organisation is required. Documentation should cover the purposes of processing data, data sharing and data retention policies and procedures.

A good starting point might be the firm's existing Data Protection Act annual registration form. However, this is only a starting point - the GDPR requirements for documentation are much more explicit than under the Data Protection Act.

Data controllers and data processors have their own separate obligations, and these are covered in more detail here - ICO guide to GDPR

There are limited exemptions for firms employing less than 250 employees, in which case documentation is only required for processing activities that:

- are not occasional
- are likely to impact the rights and freedoms of individuals; and
- involve special category data or criminal conviction and offence data.

A more detailed step-by-step guide on how to proceed with the documentation process can be found using the link above.

Other laws and regulations

As well as the necessity to comply with the GDPR, there are various other Acts and regulations in the UK which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations (PECR) 2003 - which cover 'spam' and mass-marketing mailshots. Regulations under the PECR are also issued from time to time. For example, regulations on the use of cookies on websites, and in 2016 to require anyone making a marketing call to display their number.
- Copyright Design and Patents Act - amended in 2002 to cover software theft.
- There may be other IT standards and regulations applicable to your business sector: for example, companies processing credit card transactions need to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

Sources and links

ICO home page for organisations

EU GDPR portal - www.eugdpr.org/

ICO GDPR micro site

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.