GENERAL DATA PROTECTION REGULATION (GDPR)

A Guide

JACKSON STEPHEN

ACCOUNTANTS / ADVISERS

A REAL ASSET

GENERATION DATA PROTECTION REGULATION (GDPR)

The European General Data Protection Regulation (GDPR) comes into force on 25 May 2018.

It will change how businesses handle customer information (personal data). There are some similarities between the GDPR and its predecessor, our existing UK Data Protection Act 1988. However, there are many new and different requirements.

Although GDPR is a European regulation, the UK government has confirmed that our decision to leave the EU will not affect its commencement.

Who does the GDPR apply to?

The GDPR applies to **controllers** and **processors** of 'personal data' operating within the EU. It also applies to organisations outside the EU that offer goods and services to individuals in the EU.

A controller says how and why personal data is processed and the processor acts on the controller's behalf to perform the processing.

What is personal data?

The GDPR defines personal data as *"any information relating to an identified or identifiable natural person"*. Personal data includes identifiers such as name, identification number, location data, online identifier and to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Key requirements

The GDPR contains the following key requirements:

- Personal data can only be processed if there is at least one lawful basis for doing so (for example processing as necessary for the performance of a contract).
- Another lawful basis is 'consent' (also known as 'double opt-in') - where the individual has given consent to the processing of his or her personal data for one or more specific purposes. Consent must be explicit, businesses must be able to prove consent and consent may be withdrawn.
- Some businesses must appoint a Data Protection Officer.
- Pseudoanonymisation of personal data is encouraged. Pseudoanonymisation is the process of transforming personal data in such a way that the resulting data cannot be attributed to any individual without the use of additional information - for example through encryption.
- Data breaches must be notified to a supervisory authority within 72 hours of the business becoming aware of the breach.
- Maximum fines can be up to €20,000,000 or 4% of annual world-wide turnover for infringements of the GDPR.
- A right for individuals to have personal data erased or transferred from one electronic processing system to another.

GDPR rights for individuals

Individuals have the right under GDPR to know how their personal data is going to be processed . A published privacy notice must include (amongst other things):

- Details of the data controller
- The source of the data
- Recipients of the data
- Data transfers made outside the EU
- The retention period of the data

The maximum amount of time allowed to deal with a subject access request has been reduced to 30 days under GDPR and the right to charge a fee has been removed in almost all cases.

Conclusion

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act. If you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be a starting point to build from. However, as outlined above there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

How can we help?

We will be holding a GDPR and Cyber Security Seminar for clients on Wednesday 28th February 2018. The seminar will explain key GDPR requirements and experts in GDPR and Cyber Security will share best practice.

Useful sources and links

Information Commissioner's Office (ICO) - for organisations
ICO GDPR - self assessment toolkit
EU GDPR Portal

KEY CONTACT

CHRIS MOSS

AUDIT & GENERAL PRACTICE PARTNER

D 01942 292587
M 07973 129273
E chris.moss@jsllp.co.uk

ATTENTIVE
AVAILABLE
FRIENDLY
SUPPORTIVE
ON-SIDE
PROMPT
KNOWLEDGEABLE
PROACTIVE
CARING
VISIONARY
FOCUSED
RECOMMENDED
ENTERTAINING
REALISTIC
PREPARED
GUIDING
UNDERSTANDING
INQUISITIVE
PASSIONATE
HELPFUL
SIMPLE
USEFUL
DIRECT
CLEVER
TRANSPARENT
TRUSTWORTHY
THOUGHTFUL
COMMUNICATIVE
FLEXIBLE
HONEST
ENERGETIC
PRACTICAL
RESPONSIBLE

JACKSON STEPHEN
ACCOUNTANTS / ADVISERS

A REAL ASSET

James House, Stonecross Business Park,
Yew Tree Way, Warrington, Cheshire WA3 3JD

T 01942 292500

F 01942 292501

E info@jsllp.co.uk

www.jacksonstephen.co.uk