TAIT WALKER
CHARTERED ACCOUNTANTS

GDPR
PLANNING GUIDE

INTRODUCTION TO GDPR

The new General Data Protection Regulations (GDPR) come in to force from 25 May 2018. They are a significant upgrade to the existing Data Protection regulations that have been in place since 1998. The upgrade is required to meet the developments in data use. These new developments have meant that processors of data can learn about individuals and market to them more effectively.

Simple examples are the use of cookies that track internet viewing habits or supermarket loyalty cards that record purchases. The aim is to target advertising more efficiently. However, businesses have not always explained how this works or allowed individuals to opt out. There is also a secondary market for this data where details are bought and sold without the knowledge of the individual.

The new regulations set more explicit duties for organisations that use personal data and that includes just about every business.

This guide sets out the scope of the new GDPR regime and explains the practical steps that should be taken to ensure compliance.

WHO IS AFFECTED?

All organisations are affected if they collect personal data. Personal data is any record that identifies an individual through name, address, or other contact details. This is a wide definition and shows why everyone needs to have an awareness of GDPR and how it affects their organisation.

The impact of GDPR will depend on the nature of the personal data held and why the organisation holds it. There are legal grounds for holding data and businesses that are already compliant with existing data protection law will have a head start in meeting the new rules. Any organisation active in direct marketing should already follow data protection law. However, the new rules are more demanding so organisations will have to consider data protection rules again. For example, there are specific rules for records of children and vulnerable people so the education and health sectors are a particular focus.

THE REGULATOR

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals in response to concerns about direct marketing. It has evolved over time and has the ability to issue large fines. Its remit covers all marketing channels including mail, telephone and email. There are two legally distinct areas of activity; Data Protection and the Privacy and Electronic Communications Regulations.

ENFORCEMENTS AND FINES

The existing ceiling for fines is £500,000, but this will increase to €20,000,000 or 4% of worldwide turnover, whichever is greater. Existing fines have been levied on UK business with the highest for TalkTalk of £400,000. 13 UK charities, including household names Oxfam and RSPCA, were fined a total of £181,000 in 2017.

FINES CAN BE ISSUED WHERE:

- An organisation is actively misusing the data and, as the bar on compliance is being raised, previous practice cannot be relied upon.
- There is a failure to maintain adequate controls against misuse or data loss breach. Data can be lost through hacking of websites or theft of IT equipment and a fine will follow if adequate precautions have not been taken.
- Individual rights are not protected and that individual complains to the ICO.

WHAT SHOULD BE DONE TO PREPARE FOR GDPR?

Every organisation needs to understand their responsibilities under GDPR and then take steps to make sure they are compliant by 25 May 2018 and beyond.

Below you can find a simple six key issues outline that we recommend you to follow.

1

GET AN UNDERSTANDING OF GDPR

Get an understanding of GDPR, tailored to your industry so that you understand what matters for your organisation. This is particularly important if you are working with children or vulnerable adults.

2

MAP THE PERSONAL DATA YOU HOLD

Understand what personal data your organisation holds, where it came from and why it is held. This includes electronic databases and hard copy filing. The rules aren't just for your customers; they apply to your employee data too.

3

CONSENT

Ensure you have appropriate consent processes that give individuals control of their data. This includes asking for consent, how that consent is recorded and what happens if consent is not given.

4

LEGAL BASIS

Consent is not the only legal basis for data processing. Make sure you understand the use of legitimate interests as a basis for lawful processing.

5

INDIVIDUAL RIGHTS

Understand the new rights for individuals and the ability of your organisation to meet them. This includes knowing where data is held, the deletion of data no longer needed and how you might pass data on to third parties when needed.

6

DATA PROTECTION MANAGEMENT

Review your existing data protection policy and determine what needs to improve to meet GDPR; e.g. the ability to detect, report and investigate a data breach. The policy should satisfy the letter and spirit of the law.

WHAT NEXT?

- Build your internal team; include Marketing, HR and IT
- Seek professional advice
- Read the ICO's **'Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now'** guide.