Is my business GDPR ready?

General Data Protection Regulation

In May 2018, the new EU General Data Protection Regulation (GDPR) will come into force across Europe – the legislation will apply in each of the 28 EU Member States.

This new legal framework is the most monumental change to data privacy legislation in over twenty years and will affect businesses across the globe. Any company that holds or processes the data of an EU citizen is potentially affected.

Why?

Digital advancements have resulted in consumer data being created, collected and stored within seconds. It is ever-more important to have clear laws and safeguards in place given the growing digital economy and associated cyber security risk.

What are the penalties for non-compliance?

The penalties are significant. Fines for non-compliance of up to €20m or 4% of annual global turnover could be imposed.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

HOW DOES THIS AFFECT ME AND MY BUSINESS?

Any company, anywhere in the world, that processes an EU based consumers' personal data will need to comply with the new requirements. Understanding the changes to the existing processes under the new rules is paramount. These include:

Consent – do you have explicit consent from individuals for the data you hold about them?

Under the new rules the requirements have been tightened significantly. Requesting consent from a consumer to process their personal data must be 'unambiguous'.

New responsibilities – are you a data processor or data controller responsible for processing personal data?

Under the GDPR, data processors will have greater legal liability and are required to maintain records of personal data and processing activities. There are also further obligations on controllers to ensure that any third-party contractors also comply with the GDPR e.g. cloud hosting or outsourcing.

Accountability – do you have a data protection programme and are you able to provide evidence of how you will comply with the requirements of the GDPR?

Organisational and technical measures to protect personal data are the responsibility of the data controller and data processor – data protection and privacy requirements should always be built into the development of your business processes and systems.

Mandatory breach notification – would you be able to notify a data protection supervisory authority of a data breach within 72 hours?

You will need internal processes that allow you to report and manage communications with affected consumers quickly and accurately.

New rights – do you know how you will comply with the new rights; the 'right to be forgotten', the 'right to data portability', and the 'right to object to data profiling'?

You will need processes in place to comply and reassure that these rights have been adhered to (including notifying third-parties).

Data protection officers – do you conduct large scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?

Where large scale processing of data is evident a dedicated Data Protection Officer needs to be appointed.

HOW WE CAN HELP

Our specialists can help you to assess and prepare for compliance. Through robust analysis we will identify any risks and work with you to implement processes and systems to help you comply, including:

- GDPR gap analysis
- Privacy Impact Assessment
- GDPR education and awareness sessions
- Breach management processes
- Security monitoring and reporting

GDPR comes into effect in May 2018 so it is critical to take steps now to prepare for compliance with the new regulations.

To find out more about your local RSM firm visit **rsm.global**

Alternatively, contact the Global Executive Office at our London Headquarters for an immediate response.

We will put you in touch with a Risk Advisory partner in one of our international offices who is best equipped to help with your enquiry.

RSM Global Executive Office
T: +44 (0) 20 7601 1080
E: riskadvisory@rsm.global