Your business is not ready for General Data Protection Regulation (GDPR):

Don't be the last one to comply!

The GDPR will be effective in the UK from 25 May 2018. By that date, organisations that fall within its scope will need to ensure that they are compliant. The GDPR is a European Union (EU) privacy and data protection regulation which will replace the Data Protection Directive 95/46/EC. Brexit will not affect the introduction of the GDPR.

The GDPR expands the scope of data protection laws in England, and imposes new obligations on organisations that process and control personal data. The GDPR introduces new rights for individuals and a more robust enforcement regime with fines of up to 4% of an organisation's global turnover.

EC3 Consultants

Legal insight : Business know-how

How we can help you

With so much at stake, every organisation affected by the GDPR must have a plan in place to ensure that it is compliant before the GDPR comes into force and with under a year to do this, it is important to start the process as soon as possible if you have not already done so.

Who does the GDPR affect?

It will apply to all organisations who control or process relevant personal data. Insurance companies, brokers and MGAs hold large amounts of personal data and will be widely affected.

Data controllers are organisations which determine the purpose and means of processing personal data and data processors are those organisations who carry out the instruction of data controllers.

The current regime only imposes obligations on 'Data controllers'. However, the GDPR extends these obligations and will capture data processors and cloud storage facilities and will therefore have an impact on most in our industry.

What are the key changes?

Under the new regime, notification of a breach is mandatory to the Information Commissioner's Office (ICO) and MUST be done within 72 hours and if the breach is sufficiently serious to warrant notification to the customer, the organisation responsible must do so without undue delay.

The data processor must be able to demonstrate that they have procedures in place for dealing with the obligations they owe to anyone whose personal data it holds.

Anyone can ask for data relating to them, and the data controller must provide details and/or delete without charge.

A Data Protection Officer ('DPO') will be required by all businesses that monitor volumes of data or volumes of data such as criminal convictions which is likely to include insurance companies, syndicates at Lloyd's, MGAs, and brokers.

Rules on data consent storage and use MUST be displayed and the new recordkeeping requirements are significant.

To implement these changes a new Data Protection Bill will make the UK's data protection framework fit for the digital age and give individuals more control over their data, including the right to be forgotten. It will replace the Data Protection Act 1998, putting the UK in a position to maintain the ability to share data with EU member states after Brexit.

What are the new penalties?

The GDPR will significantly increase the maximum fines on data controllers and data processors on a two-tier basis, as follows:

- Up to 2% of annual worldwide turnover of the preceding financial year or 10 million Euros (whichever is the greater) for violations relating to internal recordkeeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default.
- Up to 4% of annual worldwide turnover of the preceding financial year or 20 million Euros (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers.

New investigative powers include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises (in accordance with local law requirements).

The process

It is critical for every organisation to embed and maintain a culture which supports data protection, privacy and security through its governance and control framework by establishing reliable data protection governance. The implementation of a clear data strategy and policy which is supported by a framework of robust procedures and open communication is key.

You will need to map your current data handling practices to understand the types, locations and flow of any personal data to, within and from your organisation.

Our team have experience of working within and alongside the industry and will help with the development and implementation of data protection processes and a policy which is GDPR compliant and also meets the specific needs of your business.

We will start by:

- Assessing and mapping how data is handled across your organisation
- Conducting an analysis of the impact of the GDPR on your business
- Reviewing legal obligations under GDPR and conducting a gap analysis
- Planning a road map to compliance that fits with your needs
- Consulting and collaborating with you to determine your requirements
- Updating and developing policies as required
- Working with you to establish procedures to enable you to demonstrate compliance with your policies and procedures.

Our approach

Initiation and scoping

In the first instance, we will work with you to establish the extent to which you are exposed to the GDPR and to identify how data is currently handled across your organisation.

We will review your employee handbooks to ensure proper sanctions are included for breach and engage at board and senior manager level and develop a suitable strategy and training programme, which is likely to involve interviewing key individuals.

Findings and recommendations

Once a strategy has been agreed we will carry out a gap analysis to determine what steps are required to bring your organisation in line with the requirements of the GDPR.

Consolidation and Implementation

We will work with you to ensure that there is a clear understanding of the requirements for compliance with the GDPR at every level of the organisation. This will include developing and updating policies and procedures across your organisation. We can, where required, also provide training for your team.

Menu of costs:

Stage 1 - Fixed fee: review and audit £2,500 (2 to 3 days work)

Stage 2 - £1,250 a day as required

Annual review and audit on request.

Contact us

Sara Ager
Sara.ager@ec3consultants.co.uk
Tel: 020 3553 4898

Helena Coates
Helena.coates@ec3consultants.co.uk
Tel: 020 3553 4897

John Small
John.small@ec3consultants.co.uk
Tel: 020 3553 4874

Get in touch:

If you would like to find out more about how we can help your business, we would love to have a chat. Please get in touch:

+44 (0) 203 553 4898
info@ec3consultants.co.uk
www.ec3consultants.co.uk

@ec3consultants

EC3 Consultants
Legal insight : Business know-how