OXFORD
INSURANCE BROKERS

THE IMPACTS OF GDPR: WHAT IT MEANS FOR YOUR BUSINESS

The General Data Protection Regulation (or GDPR) is due to arrive on 25th May 2018 and represents an advancement of the existing principles within the current Data Protection Act (DPA). It is designed to protect the privacy of individuals who make their personal data available to organisations established in the EU. The GDPR will harmonise European privacy laws and govern the way organisations collect and store customer data.

WHAT IS THE GDPR?

The GDPR presents a clearly defined set of requirements for organisations who process personal data and improves the rights of individuals to have a say over how their data is used. The GDPR is designed to ensure that data legislation across the EU reflects the numerous ways that data is now used. The GDPR aims to impose stronger data security restrictions upon companies that handle personal data, and to give individuals greater transparency over where and how their personal data is used.

Compliance with the GDPR not only applies to organisations located within the EU but also to those organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. In addition to this, it also applies to all companies processing and holding the personal data of individuals residing in the EU, regardless of that company's geographic location.

WHAT TYPES OF DATA DOES THIS APPLY TO?

The GDPR applies to information that can be used to identify an individual, either directly or indirectly. This includes both:

- 'personal data', including name, identification number, location data or online identifier, and
- 'special categories of personal data' (previously referred to as 'sensitive personal data'), which now includes genetic data, and biometric data where processed to uniquely identify an individual. There will be enhanced protections over 'special category personal data', such as data relating to an individual's health.

WHAT ARE THE GDPR PRINCIPLES COMPANIES NEED TO ABIDE BY?

The main responsibilities for organisations are stated in Article 5 of the GDPR which outlines the core data protection principles.

Personal data should be:

"**a)** processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

There could be negative repercussions for organisations and individuals that breach the GDPR. These include fines of up to €20 million or 4% of the organisation's group annual turnover (whichever is larger). Significant reputational damage and personal liability could also arise.

Allocation of the fines are based on the specific articles of the Regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to lower level fines, whereas infringements of an individual's privacy rights will be subject to the higher level. In addition to fines imposed by the regulator, individuals will be able to bring about personal claims against an organisation for material and non-material damages.

WHAT ARE THE NEXT STEPS?

With the impending deadline fast approaching, all businesses that collect or process the personal information of individuals in the EU, will need to comply with the regulation. It is essential to organise a planned, structured approach to the incoming regulation changes and that senior leadership teams within the business are engaged to ensure changes are implemented at the appropriate level.

Conduct a thorough review of the existing data collection, processing and storage methods. Update existing data retention and protection policies to ensure that procedures are in place that reflect the requirements of the GDPR, Organisations must show that they have a lawful purpose for processing personal data or have the direct consent of the individual concerned.

Oxford Insurance Brokers has already implemented a comprehensive GDPR compliance plan, to ensure that the organisation's agreements, policies and processes are aligned to the GDPR.

You can visit the ICO website for more information on GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

FOR MORE INFORMATION, PLEASE CONTACT A MEMBER OF YOUR SERVICE TEAM

Oxford Insurance Brokers
6 Bevis Marks
London
EC3A 7BA

T: +44 (0)20 7283 2393
E: info@oxfordinsurancebrokers.co.uk

ABOUT OXFORD INSURANCE BROKERS

Oxford Insurance Brokers Limited (Oxford) is a fully accredited Lloyd's Insurance & Reinsurance Broker. Oxford offers a wide range of products and services to assist its clients, worldwide, with their insurance and reinsurance solutions.

Oxford, being a London based Lloyd's Broker, has access to one of the largest markets in the world. The Company has over 120 Terms of Business Agreements (TOBAs) in place with all of the major Lloyd's Managing General Agents and UK Insurance Companies. Oxford Insurance Brokers is part of the Trireme Insurance Group.

For more information visit **www.oxfordinsurancebrokers.co.uk**