# GDPR UPDATE: ARE YOU READY?

The heavily anticipated EU General Data Protection Regulation (GDPR) will become effective on 25 May 2018. The GDPR will bring considerable changes to data protection law in the UK and across the European Economic Area (EEA) more widely, and will include significantly greater fines of up to €20 million or 4% of total worldwide annual group turnover for breaches. This note summarises the need for business to consider an implementation programme and the allotment of appropriate resources to ensure compliance with the GDPR.

## Introduction to the GDPR

Personal data is defined broadly and comprises data relating to any living individual who can be identified from that data. Personal data includes:

- Names.
- Addresses.
- Social security numbers.
- Telephone numbers.
- Health information of, for example, customers and employees.

As the definition of personal data is broad there is an immense volume of personal data and this data continues to flow constantly around the UK and between the UK and other countries in the world.

Information, including personal data, can be a valuable asset and essential to making decisions. Information assets can be used effectively to meet business goals and businesses have great opportunities to exploit the information they hold for commercial advantage.

As there are significant advantages to holding and/or processing personal data most business will find themselves required to comply with the GDPR. Therefore it is important to be mindful that there are many potential ramifications if you fail to comply with the GDPR, including:

- Prosecution of or regulatory enforcement action against your business, resulting in substantial penalties of up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater).
- Adverse publicity, potentially leading to reputational damage and lost customer trust.
- Missed opportunities and wasted resources.
- A variety of sanctions in different jurisdictions.
- Increased scrutiny from data protection authorities whose confidence and powers are increasing substantially under the GDPR.
- Civil liability or punitive damages for employment-related breaches.
- Criminal liability for directors and senior managers resulting in imprisonment and substantial penalties.
- Critical system delays and failures.
- Orders issued by the Information Commissioner's Office in the UK, and data protection authorities in other key markets, that seriously impact business. Investigative powers include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises.
- Business continuity issues.
- Becoming embroiled in litigation and its attendant time, effort and expense.

The aim of the GDPR is to ensure good information handling practice. For example, identity theft, stolen credit cards and failure to comply with privacy policies may result in fraud, theft and deception. Abuse of health data, financial data or children's data can have an adverse impact on insurance, credit, jobs or parental control.

An individual has a fundamental right in the UK and across the EEA to have their personal data protected and their personal data may only be processed (that is, obtained, recorded, held, used or disclosed) under certain circumstances. This can potentially have a wide impact on businesses.

## Compliance with the GDPR

We will cover what is broadly required to comply with the GDPR below, but we strongly advise all businesses put in place a well-constructed and comprehensive programme to manage the various competing interests and act as an effective risk management tool. It is essential for compliance and to inform employees, customers, vendors, business partners, regulators and the courts of the business's commitment to data protection. We are more than happy to assist you in putting that plan together.

## Duty to know about and oversee compliance

Under the GDPR the senior management of a business has a duty to know about the content and operation of that business's compliance regime, and to oversee its implementation and effectiveness appropriately. The GDPR's new accountability principle requires data controllers to be able to demonstrate compliance with the GDPR by showing the supervisory authority (the Information Commissioner's Office in the UK) and individuals how the data controller complies, on an ongoing basis, through evidence of:

- Internal policies and processes that comply with the GDPR's requirements.
- The implementation of the policies and processes into the organisation's activities.
- Effective internal compliance measures.
- External controls.

Failure to comply with the accountability principle may result in the maximum fines of up to €20 million or 4% of total worldwide annual group turnover.

## Implementing a compliance regime

The following represents a short synopsis of what a compliance regime should encompass under the GDPR. There are of course various nuances and other requirements which we have not covered for the sake of brevity but which we would be happy to discuss with you if relevant to your business.

### 1. Data protection officer (DPO)

The GDPR requires businesses that fall within certain categories to appoint a DPO. Broadly these are:

- Where the core activities of the business consist of processing operations, which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- Where the core activities of the controller or the processor consist of processing sensitive personal data on a large scale and data relating to criminal convictions and offences.

If your business falls within one of the above categories, then you will have to appoint a DPO. Their role will be to provide the knowledge, expertise, day-to-day commitment and independence to properly advise the business of its duties, and conduct compliance activities in relation to the GDPR.

Even if appointing a DPO is not mandatory for your business, in light of the complexity of and risks associated with the GDPR, it is worth considering whether or not to appoint one anyway.

## 2. Organisational culture and chain of command

All businesses caught by the GDPR must display an organisational culture that encourages compliance and must provide staff with clear guidance and the tools that they need to achieve such a culture. It also requires that senior staff behave appropriately or are held accountable by senior management.

We recommend that a co-ordinated chain of command (in which senior management or a Chief Information Officer is designated as having ultimate responsibility) is developed, together with written reporting procedures, authority levels and protocols, including seeking and complying with legal advice.

You may wish to establish a working group, drawing on stakeholders from across the business, to take responsibility for the day-to-day management of the compliance regime.

## 3. Standards and procedures

Depending on when they were written, amendments are likely to be needed to your existing policies (in particular your privacy policy). Separate policies may be appropriate if your business collects different types of personal data for different purposes, such as marketing and recruitment. In each case, your policy needs to be accessible at every relevant personal data collection point, for example:

- Emails.
- Call-centre conversations.
- Online account and job application forms.
- Business acceptance procedures.

In particular, you should carefully review existing procedures for obtaining individual's consent as a legal basis for processing their personal data. For example, you will need to ensure that any consent obtained indicates affirmative agreement from the individual (opt in) (for example, ticking a blank box). Mere acquiescence (for example, failing to

un-tick a pre-ticked box) does not constitute valid consent under the GDPR. Furthermore, you must ensure that, once this explicit consent has been obtained, the individual can easily withdraw their consent at any time.

You must also be in a position at all times to respond quickly to any data subject's request (such as for a copy of all of the personal data held or to erase all such personal data). This is may require modifications to your technological infrastructure and organisational processes.

Other changes may be needed in certain circumstances, for example, the staff handbook regarding personal data collected from employee monitoring.

A written and comprehensive information security programme is needed to protect the security, confidentiality and integrity of personal data held. It should set out action plans for security breach, disaster recovery and data restoration.

We would also advise you to develop appropriate contractual strategies and have access to appropriate templates as a risk management tool.

Under the GDPR, you will also be required to implement "privacy by design" (for example, when creating new products, services or other data processing activities) and "privacy by default" (for example, data minimisation). You are also required to carry out "privacy impact assessments" before carrying out any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that are likely to result in a high risk to data subjects.

The GDPR also requires businesses to notify the supervisory authority of all data breaches without undue delay and where feasible within 72 hours. You should therefore carefully review your data breach response plans and procedures.

## 4. Training and enforcement

In order to minimise the risk of breaching the GDPR, and incurring the potentially significant consequences of doing so, we recommend effective compliance training programmes for personnel at all levels, including directors, heads of departments and potentially your key service providers. Bearing in mind the above factors, a formally documented training programme with employee evaluation and attendance certification will assist in demonstrating compliance with the GDPR.

To further assist with demonstrating compliance, any serious misconduct should be addressed with appropriate disciplinary action, regardless of seniority. An anonymous whistle-blowing mechanism should be considered, but legal advice should be sought before implementation in the UK and any other countries in which you carry on business.

## Regular reviews

From time to time, your compliance regime should be reviewed and updated in the light of new laws and business activities and changes to cross-border data flows.

## Conclusion

As you can see, once implemented the GDPR will significantly increase the compliance requirements and consequences of breaching those requirements. Therefore if you would like to discuss the GDPR or its requirements, or would like advice or assistance in producing and implementing a suitable compliance programme, please contact us. We would be very happy to speak with you on a no obligation basis to discuss your businesses individual needs and to put together a proposal for a suitable GDPR compliance programme.