KNIGHTS
SOLICITORS

YOUR PARTNERS IN LAW

The GDPR and the Data Protection Bill 2017

Background

The new Regulation on Data Protection ("GDPR") sets a new and uniform regime for data protection across the EU. The opening recital states: *"The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."*

The UK's implementation process for the GDPR is the Data Protection Bill published on 17 September 2017 and which is completing its Report Stage in the House of Lords. To ensure compliance with the GDPR the new Act must be implemented by 18 May 2018. Those who want to see more should refer to the website of the Office of the Information Commissioner ("ICO") which is conducting a process of consultation ending on 28 February 2018.

Most people in the UK are aware of the need for data protection and we in the UK hitherto had one of the most advanced regimes for data protection effectively enforced by the ICO under the Data Protection Act 1998. The GDPR, perhaps one of the last EU Regulations requiring direct implementation as we exit the EU, provides new rights for those whose data is held by others and responsibilities for those who keep the data and consequences for those who misuse or fail to protect it.

1. All should already be aware of the general principles of data protection but it is worth recalling what is involved using some of the new terminology. Data protection applies to both automated personal data and to manual filing systems; it is not just about computers. Both the old and new legislation require that anyone who processes personal information must comply with eight principles designed to make sure that personal information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;

- not kept for longer than is necessary;
- processed in line with your rights;
- secure; and
- not transferred to other countries without adequate protection.

Processing data under the new regime

Article 6 of the GDPR sets out the six principles which are to apply to the legal basis upon which personal data may be processed. At least one of these must apply whenever a data holder is to process personal data:

(a) Consent: the individual has to have given clear consent for the data holder to process their personal data for a specific purpose.

(b) Contract: processing is necessary for a contract between the data holder and individual concerned or as part of the process of dealing with them before entering into a contract.

(c) Legal obligation: processing is necessary for the data holder to comply with a requirement under the law (but not including contractual obligations).

(d) Vital interests: processing is necessary to protect a person's life.

(e) Public task: processing is necessary for the data holder to perform a task in the public interest or for its official functions provided this is carried out in accordance with the law.

(f) Legitimate interests: processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply to a public authority processing data as part of its official function.)

Consent

The GDPR and the Data Protection Bill attach great importance to the concept of consent. If data is to he held then the individual whose data is held must know it is being held. The ICO describes it as requiring individuals to have "real choice and control" and a "positive opt-in". If another organisation such as a third party controller is to hold information they will have to be named and consent given to the transfer of data. There is in recent guidance an explicit warning against "making consent to processing a precondition of a service".

Consent is not set in stone and can change as can the use to which data has been put as time moves one. Consent may need to be reviewed in some meaningful way and data controllers will need to keep the need for data and consent under periodic review.

Special categories of personal data

One of the main changes in data protection centres on the processing of what is known as "special categories" of personal data i.e. data which is more sensitive, and so needs more protection. This includes data in respect of:

- Race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

Special category data can only be held if strict conditions under the GDPR are met, such as obtaining explicit consent or being included in a policy.

Another highly sensitive area is the holding of information about criminal convictions. This can only be held by an employer only if this is specifically permitted by law and is covered by consent or a policy that meets the additional requirements. Public bodies dealing with this such as the Police National Computer have to maintain more stringent safeguards on the data they process – see Article 10.10).

What do I have to do to comply?

The first step to ensuring compliance with both the old and the new regimes is to ascertain what data is being held and ask yourself why? Some data may be necessary for running your business – employee's details for payroll and tax, supplier's details for marketing communication and payment, customers for taking payment and delivery. When viewed this way it is easy to see how personal data is amassed and used. Part of the duty in protecting data is to ascertain why the data is being held and to delete or destroy that which is no longer required.

One of the most important changes is the requirement for what can be called good governance requiring organisations to implement a wide range of measures to reduce the risk of a breach of data protection.

Proper implementation of the GDPR requires all undertakings including businesses to engage in some reorganisation. The first step is to decide whether or not a Data Protection Officer ("DPO") should be appointed. Even if a DPO is not required all undertakings should ensure that someone of sufficient experience and position takes responsibility for compliance with the requirement of data protection.

Risk Assessment – the practicalities

Once a DPO or person is tasked with Data Protection they need to implement an initial risk assessment. Bearing in mind that one of the main purposes of the GDPR is to reduce the incidence of breaches of data protection which in this day and age includes cyber protection. The DPO needs to consider how the information is stored and used, who has access to it. If the undertaking's data, as with many small businesses is contained on a lone

laptop – is it encrypted? Is the back-up on an external hard drive which fits in a briefcase? Leaving aside the damage to the business of the undertaking if one or both are lost because of a malfunction what is the risk if either is stolen or hacked?

The risk assessment further needs to consider what data is collected and how that information is shared. Who has access to it and why? Who has the password? How can information be downloaded – via a USB stick – how secure is this? How easily can the information be hacked? Does the machine or server holding the information have to be linked to the internet? Even if a manual system is used – how secure are the premises in which the files are stored?

In the course of reviewing GDPR compliance care is needed to ensure that even where data no longer required, it is destroyed safely. Leaving hard copy files for collection by the local authority or giving away an old laptop to charity can lead to breaches of data protection.

The action plan

Having thought about GDPR compliance the next step is to make a compliance action plan with a timeline for implementation. The need for this will be determined largely by the size of the business and what data is to be retained. For medium and larger scale undertakings there is a need to prepare privacy consents for those who data is to be retained and devise counter measures for cyber-attacks and negligent and malicious staff actions.

Data breach response programme

Equally important for larger and medium-sized undertakings are the need to prepare procedures for data breach notifications and develop a data breach response programme for prompt notification and investigation. These include handling complaints from persons seeking to enforce their rights to the necessary response to a security breach, who should be informed and what can be done to minimise any breach.

Training

Training is essential and this will again depend on the size of the undertaking. One matter worth reviewing is contracts of employment to ensure that all employees and contractors work under sufficiently strict confidentiality terms. These can provide some measure of protection to the undertaking in the event of a breach and having to answer to the ICO or any other relevant regulator of the undertaking.

Consequences

Breaches of data protection can be serious as well as reputational disasters for any undertaking. The legislation introduces a number of new criminal offences. These include, altering, destroying or concealing information to be provided to an individual through a subject access request and intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data. This could potentially have considerable consequences for the Twitter generation.

Failure to protect data can be costly. The Crown Prosecution Service was recently fined £200,000 for failure to protect data. The Deputy Information Commissioner censured a leading QC for failing to encrypt a work computer containing 6 criminal cases in which she had been retained as trial counsel, which had been stolen in a burglary from her own home. In his decision Lord McDonald noted that the maximum fine which can be imposed is £500,000. Regrettably it is only when computers are stolen or hacked (all criminal activity by others), or lost that breaches of the data protection regime are discovered. Whilst the victims may be innocent in terms of the reason the breach was discovered they are guilty of a failing to protect data as they have not taken elementary precautions such as password protection and encryption.

The penalties under GDPR have as yet to be finalised but it is unlikely they will be any less than the current regime.

Where can you get help?

The Information Commissioner's Office (ICO) is publishing practical guidance to support organisations to prepare for the change. The link is found here: https://ico.org.uk/for-organisations/data-protection-bill/

This article is correct as of 4 January 2018

About the Author

Richard Atkins attended the former Polytechnic of Central London (LLB), Kings College London, (LLM), and the former City of London Polytechnic (MA Business Law). After completing his articles with Anthony Gold, he remained there for five years before joining the Crown Prosecution Service. He served in the London Area at the Central Casework Unit Headquarters, becoming head of a special casework unit. Richard moved to the former DTI™ and HMRC™ as both a manager and special casework lawyer. He then joined Knights Solicitors after nearly 25 years of public service, becoming a Partner on 11 June 2012. Richard also served on the Law Officer's Confiscation and Delivery Board, and was a former Chair of the Whitehall Prosecutors Group on Confiscation.

In March 2012, Richard was invited by the Commonwealth Secretariat as a designated criminal law mentor to assist as a mentor in a working group appointed by the DPP of Mauritius. This was in order to make recommendations for the creation of a new asset forfeiture unit, and participate as a key speaker on a series of seminars. In 2014 and 2015, Richard was the UK delegate for the European Criminal Lawyers Association conference in Trier to protect the financial interests of the E.U.

Knights Solicitors
Regency House
25 High Street
Tunbridge Wells
TN1 1UT

www.knights-solicitors.co.uk
e-mail: knights@knights-solicitors.co.uk
telephone: 01892 537311