A concise guide to the key provisions of the General Data Protection Regulation (GDPR)

Kemp Jones Solicitors LLP
12 Basepoint Business Centre
Aviation Business Park
Enterprise Close
Christchurch
Dorset BH23 6NX

Tel: 01202 651294
Email: raynerjones@kempjones.co.uk

A concise guide to the key provisions of the General Data Protection Regulation (GDPR)

Scope of this note

The current EU data protection regime is based on a Data Protection Directive that was introduced in 1995.

Since then, there have been major advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information.

GDPR is an updated data protection law.

Businesses will have to comply with its provisions by 25 May 2018

Please see the section below - Brexit and the GDPR – for a summary of the implications of Brexit on the new regime.

We also touch briefly on the issue of Encryption – earlier this year the ICO issued new guidance on the use of encryption software to protect the security of personal data – please see **Encryption** below

Impact of the GDPR on businesses and what they should be doing now

Steve Wood, Head of Policy Delivery at the Information Commissioner's Office (ICO), in his blog "A data dozen to prepare for reform" of 14 March 2016, explained that:

"Many of the principles in the new legislation are much the same as those in the current Data Protection Act. If you are complying properly with the current law, then you have a strong starting point to build from. But there are important new elements, and some things will need to be done differently."

The ICO has published guidance on preparing for the GDPR, details of the GDPR guidance that organisations can expect to receive and when, and an overview.

Some concepts will stay the same

Some of the existing core concepts under the Data Protection Directive will remain unchanged.

For example, the concepts of personal data, data controllers, and data processors are broadly similar in both the Data Protection Directive and the GDPR.

Some concepts will change

However, the GDPR will introduce **several new concepts and approaches**, the most significant of which are outlined in the table below.

Key concepts and changes
Expanded territorial scope Non-EU data controllers and data processors will be subject to the GDPR if they operate within the EU
Dramatic increase in fines Currently, fines are comparatively low (the UK maximum fine is £500,000). The GDPR will increase the maximum fines to up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater)
Consent will be harder to obtain The GDPR requires a very high standard of consent in all cases - which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written statement. The data subject shall have the right to withdraw their consent at any time.
Mandatory privacy by design and default Businesses will be required to implement data protection by design (for example, when creating new products, services or other data processing activities) and by default (for example, minimising the amount of data collected) **Mandatory privacy impact assessments.** Businesses will be required to perform data protection impact assessments (PIAs) before carrying out any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects. The ICO will publish a list of the kind of processing operations that require a PIA. **Mandatory prior consultation** In addition, where a PIA indicates that the processing would result in a high risk to individuals, the business must consult, before any processing taking place, with the ICO.

Key concepts and changes
Registration with the ICO Instead of registering with the ICO the GDPR will require businesses to maintain detailed documentation recording their processing activities. In addition, in certain circumstances, controllers or processors are required to appoint a data protection officer.
New obligations of data processors The GDPR introduces direct compliance obligations – and financial penalties - for processors (currently only data controllers are directly in the firing line).
Strict data breach notification rules The GDPR requires businesses to notify the ICO of all data breaches without undue delay and where feasible within 72 hours unless the data breach is unlikely to result in a risk to the individuals. If the breach is likely to result in high risk to the individuals, the GDPR, requires businesses to inform data subjects "without undue delay", unless an exception applies. Data processors must notify the data controller.
The right to erasure ("right to be forgotten") Individuals will have the right to request that businesses delete their personal data in certain circumstances (for example, the data are no longer necessary for the purpose for which they were collected or the data subject withdraws their consent).
The right to object to profiling In certain circumstances, individuals will have the right to object to their personal data being processed (which includes profiling). Profiling" is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities. The fact of profiling must be disclosed to the data subject, and a PIA is required.
The right to data portability Data subjects have a new right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format and have the right to transmit those data to another controller (for example, an online service provider).

Key concepts and changes
Data subject access requests Business must reply within one month from the date of receipt of the request and provide more information than was required under the Data Protection Directive.

BREXIT and the GDPR

The GDP will be implemented in the UK before Brexit.

If the UK wants to share data with EU Member States or handle EU citizens' data, they will need to be assessed as providing an adequate level of data protection.

So, the UK is very likely to retain the legislation which it introduces to implement the GDPR

Will businesses need to make major changes?

Yes.

Such changes may include redesigning systems that process personal data, renegotiating contracts with third party data processors and restructuring cross-border data transfer arrangements.

These changes will take time to implement so businesses should plan ahead.

Encryption

The ICO has published new guidance on the use of encryption software to protect the security of personal data.

The Data Protection Act 1998 (DPA) does not specifically state that organisations must encrypt personal data.

However, the seventh data protection principle requires organisations to take appropriate technical and organisational measures to keep the personal data they hold secure.

Peter Brown, a Senior Technology Officer at the ICO, has stated in a blog, *"Encryption, being a widely available technology with a relatively low cost of implementation, is one such measure. The ICO takes the view that regulatory action may follow in cases where a lack of encryption has led to a loss of data. A significant number of the monetary penalties we have issued since 2010 relate to the failure to use encryption correctly as a technical security measure. Where data is not appropriately secured, loss, theft or inappropriate access is much more likely to occur. On top of the fines, data controllers risk significant damage to their reputation if they do not store personal data securely."*

The guidance features several scenarios designed to help organisations consider when and how they should encrypt personal data.

For example, transferring personal data by CD, DVD or USB, sending personal data by email or fax, or storing personal data on devices such as laptops, mobile phones, back-up media, databases or file servers

As regards collecting data, if personal data is in any way sensitive or otherwise poses a risk to individuals (for example because it includes credit card numbers), collection would only be sufficiently secure with the use of a secure, encryption-based transmission system.

This data should also be held on a server properly secured by encryption or similar techniques.