SLAUGHTER AND MAY

Key facts on the GDPR

This publication is the second in a series of briefings on the General Data Protection Regulation (the 'GDPR'), which was provisionally agreed on 15 December by the European Parliament and the Council of the EU. It provides an overview of some of the key changes the GDPR will introduce.

A wider extra-territorial scope
The GDPR will now also apply to controllers established outside the EU that offer goods and services, including free of charge, to individuals in the EU or that monitor the behaviour of such individuals.

Current principles remain but new concepts and rights introduced such as:

- accountability – which requires data controllers to be able to demonstrate compliance;
- privacy by design - which requires data controllers to consider privacy risks at the outset of any new project;
- new or codified rights for individuals – e.g. data portability and right to erasure.

Mandatory data breach notification to the data protection regulator without undue delay (i.e. 72 hours where feasible) unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals.

Changes to the ways in which personal data is collected and used. Additional information will need to be communicated to individuals. Consent must be "unambiguous" or "explicit" in some cases (such as profiling or international transfers).

Direct obligations on data processors - e.g. maintaining records and putting in place appropriate security measures. There are also additional requirements to include in data processing agreements.

Stronger sanctions, in particular competition-style fines of up to 4% of annual worldwide turnover or 20,000,000 Euros, whichever is highest.

A more harmonised EU data protection regime, including increased co-operation and consistency between EU regulators and a 'one-stop-shop' for controllers.

Data protection officers
to be appointed by controllers and processors in certain circumstances such as when their core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale.

International transfers.
No radical rethink of the provisions on international transfers. Transfers to foreign courts or administrative authorities (for example in the context of litigation or global investigations) are likely to be harder to justify.

Notification system.
Data controllers will no longer be required to notify/register with their local data protection authority.

Timing.
The GDPR is expected to be formally approved in March/April 2016. It will apply directly in Member States two years after that.

Practical steps
Organisations should be looking to obtain board buy-in to secure the resources and support necessary to design and implement an effective compliance strategy. See our first briefing: A new era approaches for European data protection (available on our website).

February 2016

OSM0006961_V04