MACFARLANES

THE NEW EU DATA PROTECTION REGULATION

DATA PRIVACY

It will not have escaped your attention that the EU is currently debating the final text of a new EU-wide Data Protection Regulation (the Regulation). The Regulation will replace the Data Protection Directive 95/46/EC which is implemented in the UK by the Data Protection Act 1998. The final text of the Regulation is unlikely to be agreed before the end of 2013 and unlikely to come into force before the end of 2015 but there is plenty that businesses should be considering now to prepare for the major changes introduced by the new Regulation.

The passage of the Regulation through the legislative process has received unprecedented interest and the Regulation has been subject to intense lobbying by businesses, privacy campaigners and other interest groups. Perhaps the most controversial measures being debated concern the "right to be forgotten" and the removal of the ability to justify processing by implied consent.

Until we know the final text of the Regulation, the full implications remain uncertain but this note draws out four broad themes. We also consider what businesses should (and should not) be doing now in preparation for the new Regulation.

FOUR THEMES

1. More internal compliance

There are a number of specific proposals, which will make work for internal compliance and legal teams:

- All private sector organisations with over 250 staff and some smaller high risk data businesses will be required to appoint a **data protection officer** to be responsible for data protection compliance. There is a suggestion that data protection officers will have enhanced employment protection.

- The annual obligation to register with the Information Commissioner will be replaced with an obligation to keep **internal documentation**. The Regulation currently grants delegated powers to the European Commission to specify the exact requirements; if more detailed documentation is required then this could significantly add to the existing regulatory burden.

- **Data security** breaches will have to be notified both to the Information Commissioner and possibly to the data subject. Whilst the draft Regulation currently contains no *de minimis* exception and imposes an unrealistic timetable (with notifications having to be made within 24 hours) we expect that this proposal will make it through in some form. This is significant because most of the recent monetary penalty notices issued by the Information Commissioner have resulted from data security breaches and some as a result of (voluntary) notifications.

- Data controllers will be required to verify, by way of an **internal or external audit**, their data protection practices.

- Formal **risk assessments** may be required and there will be a new concept of **data protection by design** requiring businesses to take privacy into account when designing new products and services.

2. Easier international data transfers

- **Binding corporate rules** will be explicitly recognised as a means of managing international transfers. A single supervisory authority will approve the binding corporate rules on an EU-wide basis. This will stream-line the process, but with associated powers delegated to the EU Commission, pragmatism cannot necessarily be guaranteed.

- The use of **EU Model International Data Transfer Agreements** will be expressly recognised. Member states will not be able to impose additional requirements.

- An express EU-wide exception for **small scale ad hoc transfers** whether the transfer is not "frequent or massive".

3. Large fines and more robust regulators

- The headlines have been grabbed by the prospect of antitrust style fines of up to **2 per cent of global turnover** (not profit). The draft Regulation also envisages that fines would be imposed in respect of what might appear to be relatively minor breaches. The exact details may be changed but it is clear that there will be **meaningful sanctions.**

- Historically the UK Information Commissioner has been relatively pragmatic in his approach to regulation, interpretation and enforcement. The new Regulation introduces the idea of a "one stop shop" so that a business is regulated in its home state, but subject to a series of **consistency measures** by regulators in other member states. This demonstrates a clear intention that EU privacy rules be enforced much more uniformly: the UK may lose the benefit of past pragmatism.

- Finally in no less than 26 places, the draft also delegates substantial powers to the European Commission, which could well lead to the introduction of a series of **unwelcome secondary measures**.

4. Increased scope

- The new Regulation will expressly apply to **data controllers headquartered outside Europe**.
- The Regulations will **apply to processors** as well as controllers. The need for commercial contracts to get the balance right between processors and controllers is critical. If the processor acts outside its authority, then it becomes liable to the full impact of the turnover based fines. Businesses will need to review and update their existing outsourcing and other commercial agreements.
- The definition of sensitive personal data will be extended to **genetic data**, meaning that explicit opt-in consent will generally be required.

WHAT SHOULD YOU BE DOING NOW?

If you have not already done so, carry out a comprehensive **data mapping** exercise to understand how your business is processing data:

- Generate a written document that captures, on an ongoing basis in a central repository, what data your business has (including outsourced processors) and how your organisation processes it. In generic terms, you should be able to describe **what you collect, how you collect it, where is it stored** and **how is it protected**.
- Establish an interdepartmental team – IT, marketing, HR and finance – that has sight of all the data and processes in the business and how the business is changing.
- Try to create a diagram that shows the main data flows in and out of the organisation and the main data repositories.
- This is a time consuming task but is the key to getting your risk management process right and will allow you to instruct external advisers efficiently, with focus and certainty.

Ensure that **data security is a business priority**:

- The draft Regulation does not change the legal standard of care (although the draft Regulation would introduce a formal requirement to carry out a data security risk assessment). The vast majority of large fines to date have related to **data security breaches** and many businesses have work to do in order to comply with the existing law.
- Data security is partly a technical issue, but is also an organisational issue with many workers knowingly violating corporate security policies and others still using unencrypted files and memory sticks. "Bring your own device" is just the latest high profile issue where a combination of good IT security and sensible HR policies can reduce risk.
- Think about resourcing and how to access **data privacy expertise**, whether that is in-house or externally. Regardless of whether or not the final text of the Regulation contains a mandatory requirement to have a data protection officer, privacy compliance professionals with the requisite experience are already in short supply and you might wish to start looking before everyone else.
- Do **not** spend time now updating your privacy policies. The draft Regulation expressly requires policies to use clear and plain language but is prescriptive about content. It is better to wait until the final text of the Regulation is known before rushing to make changes now.
- Compliance with the new Regulation will require **additional resources** and budgets for the next two-three financial years should reflect the additional expenditure required. Whilst the Regulation is unlikely to come into force until the end of 2015, we expect that larger or more complex data businesses will need all of the expected two year implementation period and so budgets should be set accordingly.

CONTACT DETAILS
If you would like further information or specific advice please contact:

RUPERT CASEY
PARTNER
DD: +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

DANIEL POLLARD
SENIOR SOLICITOR
DD: +44 (0)20 7849 2200
daniel.pollard@macfarlanes.com

MAY 2013

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT
T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com