CROWN RECORDS MANAGEMENT

EUROPEAN UNION (EU) GENERAL DATA PROTECTION REGULATION – IN A NUTSHELL

What is the EU General Data Protection Regulation and why is it being brought in?

The EU wants to reform data protection and cut red tape for businesses across Europe by bringing in a single set of rules. In future there will be one single Data Protection Authority (DPA) responsible for each company, generally reflecting where its headquarters are based. The Regulation also aims to protect the rights of European citizens to have control over their personal data.

So, is it a change in legislation?

No, because it is a 'regulation' rather than a 'directive' there is no need for a change in legislation in any country. The regulation simply sets out a joint agreement of how data protection is to be managed.

Who will it affect?

Any business that operates from within the EU, does business with companies inside the EU, stores its data in EU member countries or handles the personal data of European citizens.

When is the Regulation expected to come into force?

It's a question with no definitive answer, although the stated timescale is for ratification by the end of this year and implementation in 2017.

In reality it may well be 2016 before politicians can agree on a final draft. But what is clear is that significant progress is being made and the underlying principles have been agreed – so there really is no reason for businesses to put off preparations any longer.

What's been happening at the EU in recent months?

The EU Council took a significant step to pushing through the Regulation by reaching partial agreement on some aspects of the draft in March 2015, particularly in relation to its 'one-stop shop' mechanism and principles of protecting personal data.

The desire for lawful, fair and transparent data processing and, importantly, for EU citizens to have more control over their data is pretty much unanimous.

The Council also re-iterated its aim to 'create a more rigorous and coherent data protection framework in the EU, backed by strong enforcement' and to 'put individuals in control of their own data'.

What happens next?

EU ministers will meet again in June with a view to finalising the details. EU Justice Commissioner Vera Jourova has even Tweeted "we may be on track for conclusion in 2015". Although her view has been described as optimistic by many politicians it would be a major surprise if the Regulation, following a two-year implementation period, is not in place by 2018 at the latest.

What will be the most challenging aspects of the Regulation?

With so much focus on how the data of European citizens is stored and handled, businesses will face a serious challenge to get their processes in order.

To begin with, they will need the specific and freely-given consent of data subjects to collect data in the first place. Data must be accurate and up-to-date. The policy of 'privacy by design' means data protection should be at the heart of all processes.

Citizens will have the right to view their data and ask for it to be edited. The 'right to erasure', will add further complications as companies will be expected to find and edit large amounts of data quickly – and will need processes in place for data subjects to make those requests.

The threat of data breaches will no longer be a concern just for data controllers but also for data processors as huge fines are introduced across the board.

The Regulation requires companies with more than 250 employees to appoint a Data Protection Officer. Smaller companies which hold more than 5,000 personal data records will have the same requirement. For many it may be more sensible to outsource this post; but the financial implications of the new Regulation will also be a concern.

What will the consequences be for those who fail to comply?

Huge fines, up to 100m Euros or five per cent of global turnover, for companies that deliberately or negligently breach the Regulation are included in the draft. In future, data breaches are going to be very expensive – and lead to serious loss of reputation. It could be make or break for many UK companies.

There will also be requirements for businesses to report a data breach quickly. That time frame looks likely to be set at 72 hours, which will be a real challenge for businesses that have not set up adequate processes.