NEW EU DATA PROTECTION LAW: TIME TO START PREPARING

Posted on 08/07/2014

Category: Uncategorized
Tag: cat-compliancenews

A survey shows that, if you're confused about the proposed new EU data protection laws, you're not alone. However, if you use or collect personal data you should be aware of three points – the new law is coming, it will affect your
business and it could well involve significant costs.

A survey shows that, if you're confused about the proposed new EU data protection laws, you're not alone. However, if you use or collect personal data you should be aware of three points – the new law is coming, it will affect your business and it could well involve significant costs.

What should businesses do now in order to prepare?

- Make sure that budgets and planned financial forecasts for 2015-2017 include provision for compliance with the new law (including the appointment of "data protection officers"). See below for an explanation of why costs are likely to be significant.

- As regards IT systems and business processes (particularly in e-commerce), keep in mind that when the new law comes into effect, methods for obtaining consent for personal data use may need to be changed and steps will need to be taken to facilitate both portability and permanent deletion of data (see below). In some cases, it may be better to wait until there is greater certainty before proceeding with major new systems-related commitments; where that is not practical, try to ensure that systems have some flexibility to meet changing conditions and make provision for possible additional implementation costs.

Background

In May 2013, the UK Information Commissioner's Office (ICO) published a survey of 506 people who described themselves as having responsibility for data protection where they worked. Not one of them could accurately answer all of the questions about the requirements of the proposed new data protection laws that are currently expected to come into force in 2016. Crucially, few respondents appeared to have a clear picture of the implications of the reforms for their business – although in some areas this is not surprising given the lack of clarity in the drafting of the proposals.

What are the proposed new laws?

At present, UK data protection obligations are primarily governed by the Data Protection Act 1998 (DPA), which implements an EU Directive. The European Commission's proposals for reform are the subject of fierce debate and may still change; in particular, they must be agreed by both the European Parliament and EU Member States, which is likely to result in at least some significant amendments. However, if they come into force as originally proposed by the European

Commission, the implications are likely to include:

- Even more problems with consent: Subject to some exceptions, consent of individuals is generally needed in order to process their personal data lawfully. It has proved difficult for many businesses to develop practical methods of compliance, particularly online (as illustrated, for example, by difficulties over internet cookies). However, instead of seeking to simplify this problem, the draft Regulation proposes to raise the bar for consent so that it must be "explicit" in all cases, regardless of context. This will almost certainly make it even more difficult for businesses to be confident of having achieved compliance.
- Significantly more red tape: At present, businesses are free to adopt a risk-based approach to compliance. However, under the proposed Regulation, detailed records documenting compliance measures would have to be maintained at all times, regardless of the actual risk to personal data (failure to do so could lead to a fine). Both data controllers and data processors will have to appoint internal "data protection officers" to oversee and monitor compliance and the ICO will have to be promptly notified in the event of any data security breach (again, regardless of the risk involved). There will also be updated rules on the transfer of personal data outside the EEA. The ICO has criticised the Regulation for putting "too much emphasis on mandating the bureaucracy of data protection when the objective... is the protection of personal data in practice rather than the creation of paperwork."
- New requirements for deletion of data and portability: Individuals will have a new "right to be forgotten" i.e. to insist that certain data about them is deleted (more recent drafts suggest that EU legislators prefer the term "right to erasure"). Individuals will also have a new right to demand a file of their personal data in a format which can easily be transferred to anotheR service provider, such as a social media platform. Businesses will have to set up new processes that facilitate these rights – and there is considerable uncertainty over what steps they will be obliged to take in practice.
- Data processors will have to comply: Businesses which process data on behalf of others will, for the first time, be subject to direct obligations under the new law.
- Significantly higher fines: Fines for breach would be increased to up to €1 million or 2% of

worldwide turnover (at present the maximum fine under the DPA is £500,000). The European Parliament favours an even higher level of fines, although it remains to be seen whether EU Member States will agree to this. To date, the majority of fines have been imposed on public bodies, rather than the private sector.

What will compliance cost?
Estimates of the possible cost/benefit are the subject of much debate. Whilst the European Commission projects overall benefits, the UK Ministry of Justice has suggested a net cost to UK businesses of £80-320 million per year. Our view is that, compared with the existing regime (and leaving aside questions of wider social benefits), there are likely to be significant additional costs for business, including:

- a substantial one-off cost from the need to revise compliance procedures, redesign IT systems such as customer/service user databases, CRM systems and e-commerce software and review/update legacy data to meet the new requirements outlined above – particularly the new definition of consent, data portability and "the right to be forgotten/right to erasure"; and
- increased ongoing costs as a result of a significantly more onerous and bureaucratic regulatory regime (see above).

What is the timetable?
The proposal needs to be approved by both the European Parliament and EU Member States. Whilst it is hoped that an agreement can be reached by the end of 2014, there is a reasonable likelihood of negotiations extending into next year. There is also expected to be a transitional period before it takes effect. Assuming that the legislation is adopted later this year or next and the transitional period is as envisaged in the original proposal (i.e. 2 years), this means that it would be in force by 2016 at the earliest and 2017 at the latest.

Why start planning now?
Other EU Member States besides the UK are known to be concerned about the proposals, which may lead to changes. It may therefore be tempting to wait until the shape of the new law is clearer before making any contingency plans. However, if you wait too long, there may be insufficient funds in budgets to cover the cost of implementing the necessary changes or insufficient time to make any necessary changes in the most cost-effective way.
If you are going to wait, you need to consider how long to wait for. It may be fine to put things off if agreement on the Regulation is reached relatively quickly – but if the process takes longer, it could be next year before a final text is published. Even that may not resolve all of the uncertainties outlined above – because important matters of detail may only be dealt with in secondary legislation or guidance, which is not likely to be finalised until some time after the Regulation is adopted (potentially leaving very little time to prepare).
For many businesses, however, waiting is not an option – because, for example, replacement of an ageing IT system cannot be put off any longer without putting business-critical functions at risk. Where that is the case, try to ensure that systems have some flexibility to meet changing conditions and make provision for possible additional implementation costs.

If you would like to discuss any of the issues raised in this article, please speak to one of the contacts listed below:

Dan Reavill
Partner, Commercial, IP and Technology
+44 (0)20 7295 3260

Alistair Wilson
Consultant, Commercial, IP and Technology

+44 (0)20 7295 3345

Louisa Chambers
Senior Associate, Commercial, IP and Technology
+44 (0)20 7295 3344

Travers Smith LLP
10 Snow Hill
London
EC1A 2AL
T: +44 20 7295 3000
F: +44 20 7295 3500
www.traverssmith.com