RegulatoryStrategies

RADICAL SHAKE-UP IN DATA PROTECTION LAWS...

...but good news for your data protection officers!

Following a number of leaked drafts, the European Commission published its proposals for reforming the EU data protection regime on 25th January 2012.

Subject to these proposals being accepted they will replace the current European Data Protection Directive 95/46/EC and the country-specific data protection legislation across all 27 Member States - in the UK, the Data Protection Act 1998 (DPA). And this could be as early as 2014/15!

Mike Bradford, BIIA's Advisor on Privacy and Data Protection, provides a summary of key impacts:

Initial reaction to the proposals has varied. Reaction in the UK by privacy specialists and businesses alike has been one of concern around the breadth and depth of the changes. Our regulator, the Information Commissioner (ICO), is supportive of some proposal but not others and is concerned at how some can, in practice, be enforced - for example taking action against non-UK organisations that breach the Regulations in the UK.

The CBI has suggested that it will stifle innovation. Businesses - and the credit industry - are already struggling with a heavy regulatory burden and commentators - including this one - consider that it elevates data protection to the level where it needs to be taken seriously by chief executives and corporate boards, as opposed to technical compliance staff. A recent article suggested that it is a good time for data protection officers to submit that long overdue request for a pay rise!

So what will all this mean for the UK credit industry?

The Commission hopes that the Regulations will help business in three ways. Firstly, they should create legal certainty. Secondly, they should simplify the regulatory environment with organisations only having to deal with a single regulator and the need for notification being dispensed with. And thirdly, they should provide clear rules for international data transfers. But do they?

RegulatoryStrategies

The first thing to note is that the proposals that will impact businesses are in the form of a Regulation rather than a Directive. The Regulation will be enforceable in all Member States two years after it has been adopted. Unlike a Directive the Regulations will have immediate and direct impact on UK organisations - and possibly within 2-3 years. Being a Regulation, while one set of rules is meant to be beneficial to organisations operating internationally, those who are used to dealing with the reasonably practical obligations of jurisdictions such as the UK could face a cultural and legal shock. The compliance bar has gone up. The principles and obligations for all organisations – including those operating in the credit sector - are far more prescriptive in nature than under the DPA.

But everything is not totally new and the credit industry should not forget that its fair obtaining clauses and data retention periods negotiated over many years with the ICO could still meet the requirements of the Regulations once the headlines of 'explicit consent' and the 'right to be forgotten' have put to one side. Similarly the 'data protection principles' in the Regulations are very similar to those familiar to UK organisations under the DPA - for example data retention, accuracy and relevance.

There are also similar provisions as already contained in the DPA around direct marketing, data security and the appointment of data processors as there are around specific types of data for research, employment and health.

As ever the devil is in the detail and some of the hysteria about debts having to be deleted in the credit press should be taken in the context of the carve outs already in the Regulations.

The following is a high level commentary of the principal changes and their impacts:

- **New fining powers** will determine a fine based upon the nature of the breach. Maximum fines will be up to €1m or 2% of global turnover. The financial impact will be far more significant in some geographies like then UK where fining powers are currently capped.

- Representative bodies will be able to bring **collective action** on behalf of a number of individuals. Similar to Class Actions in the US, this opens up organisations to actions by a powerful or vociferous group of customers or individuals in the event of breach. Perhaps a charter for giving more power to some of the anti-credit industry lobbies?

- Organisations will have to **notify the regulator of a data breach within 24 hours** if feasible and, where individuals are adversely affected also notify them without 'undue delay'.

  This is a major departure for UK organisations where in most cases notification is not compulsory. However both the ICO and Which? have been lobbying for this for some time.

  In practice, for organisations and businesses:

  - There will be an expectation that a demonstrable and documented incident management plan is in place and that employees have received sufficient training to be able to deploy the plan; and

  - An assessment process will need to be developed to enable to organisations to quickly assess whether personal data has been lost and whether individuals are likely to be impacted.

- All data **processors will be obliged to document details of processing and can be sued for a breach of this regulation**. This will extend to all uses of personal data held in databases, used in products and transferred to third parties.

  This liability on data processors is a radical departure from the current Directive (and DPA) where data processors have no prima facie liability for data protection in respect of the data they process for their client, the data controller.

- If a **data processor processes data outside of its instructions from a data controller, it will become a data controller in its own right**.

  Data processors will need clearly defined instructions from data controllers in order to ensure it does not become the data controller.

  As a result of this new liability and potential liability on data processors it will be incumbent on both parties to ensure very clear contractual wording stating the precise boundaries and limits of the processing required.

  It is also likely that data processors will be take a more proactive role in contract negotiations to protect their position.

- **Consent must now be 'explicit'** and can be withdrawn. The onus for proving consent rests with the data controller. Consent from a child needs to be authorised by a parent or guardian.

  But in many cases 'consent' is not the provision relied on by organisations in the UK to make the processing fair and lawful - for example the 'legitimate interests' provisions of the DPA enable many organisations to comply with this requirement on a 'balance of interests' test subject to transparent notification. This is in effect how credit reference agencies in the UK and credit grantors process data.

  The expectation of consent being 'explicit' means that a more positive indication of the customer's agreement may be required than, for example, merely continuing with the transaction.

  In practice, for organisations and businesses:

  - Consent clauses will need reviewing and potentially revising to comply.

  - Processes and communication need to be introduced to allow individuals to withdraw their consent for processing.

  - Where a data controller processes data relating to children, they will need to ensure that they have sufficient information to establish whether someone is under 18 and to be able gain authorisation from and authenticate a parent or guardian. This may impact some Authentication products in the UK.

- Any organisation with more than 250 employees must appoint a **data protection officer** (DPO). Any public body must appoint a DPO irrespective of size.

  The DPO can be appointed for 2 years and re-appointed thereafter. They can be an internal member of staff or an external advisor on a service contract. The Regulations outline specific duties and responsibilities of the DPO.

  Organisations will need to review the skills and remit of their data protection people and may need to consider using an external independent resource in tandem with the internal appointment to ensure this independence and requisite skill-sets.

- **Privacy impact assessments** will need to be carried out for certain types of processing.

  Organisations will have to have a process to carry out a privacy impact assessment where required and staff who are trained in assessments.

- Organisations will have to be able to **demonstrate that processing activities comply with data protection law**.

  Data processing activities will need to be documented and evidence the measures taken to comply with data protection law - this will require more detailed action-orientated policies at both strategic and operational level. The documentation must also detail all processing carried out by the organisation and details of data processors.

- A reinforced **'right to be forgotten'** is designed to enable people to manage data protection risks online and to be able to delete their data if there are no legitimate reasons for retaining it.

- People will have easier **access to their own data** and be able to transfer personal data from one service provider to another more easily.

- People will be able to refer cases where their data has been breached or rules on data protection violated to the **data protection authority** in their country, even when their data is processed by an organisation based outside the EU.

There is an increasing amount of activity both here in the UK and across Europe to raise specific issues that business - and indeed some consumer groups - feel need to be diluted or even tightened up.

It is never too early for the credit industry to start to plan. But this now needs to be strategic rather than operational - which is typically where data protection has fitted in. As one commentator has said, this lifts data protection to the same level as antitrust and competition law. If UK organisations ever needed an incentive to invest in data protection expertise they have been handed one!

Mike Bradford is Founder and Director of Regulatory Strategies. He can be reached at: mike.bradford@regulatorystrategies.co.uk
www.regulatorystrategies.co.uk