Countdown to radical data protection changes...they are now here

After 3 years of lobbying and discussion, the new EU data protection Regulation was agreed on 15th December.

The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. On 15th December 2015 an agreement was found with the European Parliament and the Council, following final negotiations between the three institutions (so-called 'trilogue' meetings).

The full EU press release can be found at http://europa.eu/rapid/press-release_IP-15-6321_en.htm. This also contains headline changes to our current data protection regime.

Following political agreement reached in trilogue, the final texts will be formally adopted by the European Parliament and Council at the beginning 2016. The new rules will become applicable two years thereafter.

What this means for the credit industry is that within two years, the current Data Protection Act will be replaced by the new EU Regulation.

Unlike an EU Directive, an EU Regulation must be transposed into each member state's legislation exactly as drafted with no room for interpretation or amendment at country-level.

The aim of the Regulation is to harmonise EU data protection law to support the single market agenda.

The current model, with 28 member states each having their own legislation based on the Data Protection Directive (95/46/EC) but with very different local interpretation, sanctions and enforcement provisions, was perceived to be a barrier to achieving a single market as organisations and consumers were faced with 28 country-specific versions of the Directive as transposed into national legislation – in the UK, through the Data Protection Act 1998.

Essentially the compliance bar for UK organisations has moved up closer to the German model and there will inevitably be compliance and business challenges to prepare for the new Regulation - subject of course to the UK remaining part of the EU. Even if the referendum vote were for the UK to leave the EU, it is not uncommon for those European countries which are not members of the EU to adopt similar legislation to their EU counterparts to facilitate cross-border trade.

Having reviewed the current text - over 200 pages - the key differences from the current Data Protection Act regime include:

1. Joint obligations and liabilities for data controllers and data processors.
2. Mandatory data protection officers for most businesses where personal data are key to their operations – but this can be outsourced to an expert DP advisor.

The requirements for the role are strict and set out in the Regulation and there must be no conflict of interest with the job-holder who must have access to senior management / Board. Our advice is to address this requirement now, which can be fulfilled either internally or by appointing an external consultant. Regulatory Strategies is already in discussion with a number of clients on the latter option.

3. Mandatory data breach reporting to the regulator and to the affected consumers
4. Mandatory policies, procedures, plans – and testing of data breach plans
5. The relevant regulator will be where the main business office is established
6. The Regulation applies to non EU businesses targeting goods or services at EU consumers
7. The bar for consent has gone up requiring the consumer to take positive action to demonstrate consent
8. Consent must be obtained for profiling
9. The requirement for notifying the regulator of processing activities is removed
10. Processing a child's data on-line requires parental consent if the child is below 16 (Member States can take down to 13)
11. Subject access response time is reduced to a max of one month and will be free of charge
12. A 'right to be forgotten' has been introduced BUT is limited to where there is justification for the consumer
13. A right to data portability has been introduced enabling the consumer to require a data controller to pass their personal data to another data controller
14. Data protection by design and by default are now legal requirements ie systems and products must be built from the bottom up around privacy, and the 'default' position must only be to collect sufficient data for the precise processing involved
15. Privacy Impact Assessments must be carried out and evidenced where new technologies are being deployed
16. Increased fines of up to 4% global turnover

Our strong advice is that you should be auditing your current data protection compliance now – if you have a clean bill of health at this stage the migration to the new requirements should fit into 'business as usual' rather than detract from your everyday commercial activities. Without this advanced planning the much more onerous obligations – and significant penalties for non-compliance – will materially impact your business. Approach it in as you have FCA regulation.

In particular, we would suggest you address the following:

- Incident management plans should be in place. Data breach reporting is not currently mandatory in the UK but the new Regulation will require businesses to notify both the

regulator and affected customers. It will therefore be essential to move quickly and without a plan in place, it is likely that wrong decisions will be made.

The recent Talk Talk hacking incident highlights the amount of potential adverse publicity that a data breach can cause – it also shows that an organisation needs to be able to demonstrate that it has sufficient security in place to prevent breaches and, if they do occur, are able to protect their customers and address gaps. It is also essential to be able to effectively communicate with the press and media should an incident get into the public domain.

- Policies and procedures will no longer be a 'nice to have' – data controllers will have to have these in place so checking that data protection policies, privacy statements etc. are in place and are sufficiently robust is essential. Previous action by the Information Commissioner's Officer has already shown that just having procedures and policies in place is insufficient – staff need to be fully trained and aware of their responsibilities.

- The Information Commissioner's Office already recommends the use of Privacy Impact Assessments / Privacy by Design in the development of any new product or new use of data. Again, this will become a requirement and a documented process will need to be in place.

- You should already have robust contracts in place with Data Processors to ensure that they are meeting your data protection obligations. The future will see Data Processors facing their own data protection obligations so it is likely that clauses in contracts will need to reflect this.

The above highlights a few key areas that are likely to impact on businesses. Taking action now will help to ensure that businesses and staff are prepared for the changes. And – as with our preparations for the FCA regime – if we leave things until the last minute all focus will be upon meeting the regulation rather than developing our businesses.

Mike Bradford
Helen Lord
Regulatory Strategies Ltd
www.regulatorystrategies.co.uk
consultancy@regulatorystrategies.co.uk