RegulatoryStrategies

BIIA
Business Information Industry Association

THE EVOLVING DATA PROTECTION LANDSCAPE

Take action today to prepare for tomorrow……

The global, EU and UK data protection landscape is at a crossroads. And organisations across all sectors are waking up to the fact that change is inevitable.

Here Mike Bradford, founder and director of Regulatory Strategies and BIIA's expert advisor on privacy and regulatory affairs provides a summary of what he - and many other expert data protection commentators and practitioners - feel should, and indeed **must**, be on the strategic radars of organisations **now** to ensure they are in good shape for the challenges that will come under new EU Regulations.

WILL THE PROPOSED EU DATA PROTECTION REGULATIONS BE ENACTED OR LOSE IMPETUS AND DISAPPEAR DURING THE LENGTHY EU LEGISLATIVE PROCESS?

Quite simply, the Regulations will happen. It is inevitable that there will be change - and significant change to the data protection laws we have become familiar with in the UK and Europe under the 1995 Directive.

And if the Regulations remain as currently drafted, the UK will move closer to a bureaucratic, detailed and prescriptive data protection regime - and one that our own regulator, the Information Commissioner, takes issue with.

To demonstrate the national differences across EU member states, the German approach - which is seen by many as the model on which the Regulations have been drafted - has been cited as being: 'trust is good; but control is better'. And the Rapporteur charged with taking the Regulations though the EU legislative process, Jan Albrecht, is himself, perhaps by no coincidence, from the German Green party.

The real question is not 'if' but 'when?'.

The committee stage, already underway, led by LIBE (Civil Liberties, Justice and Home Affairs) will shape the speed of the Regulations as will 'political' considerations, with certain key individuals, notably Viviane Reding, EU Vice-President and Commissioner for Justice responsible for introducing the Regulations in January 2012, who will want to see a conclusion during their term in office.

We see the remainder of 2012 (and subject to any delays, early 2013) as being a critical period as the European Parliament will propose what should be a revised draft from that tabled in January this year.

If the process goes to schedule we would expect a LIBE Committee Hearing and presentation of the draft Regulations in plenary before the end of 2012 with 2013 and 2014 seeing ongoing three-way discussions between LIBE and other 'Opinion Committees', the Council and Commission.

Summer 2014 is the likely time by which we will know what the final Regulations will look like, with a further 2 years to implementation by all member states.

And because we have Regulations rather than a Directive, there will be no room for 'interpretative drafting' at member state level - the Regulations must be enacted as written, unlike the Data Protection Act which is based on, but does not replicate verbatim, the Data Protection Directive.

The Commission's top priority is to move away from different approaches to the current Directive's implementation and interpretation to a single set of rules on data protection valid across the EU - the new Regulations.

And a final 'sting in the tail' are the 26 delegated acts in the Regulations whereby it will be the Commission that effectively has a drafting function even after the Regulations have been finally approved.

SO WHAT ARE THE KEY CHANGES?

Fundamentally the Regulations are far more challenging for organisations to understand and adapt into business practice than the current Directive.

The Regulations are at least twice as long as the Directive and are more detailed and prescriptive**. And our opinion - and we are certainly not alone in this - is that the final Regulations will be even longer as they will contain new qualifications and exceptions to the general rules - which we suspect are unlikely to be significantly changed**.

We see the way through many of the current concerns - for example the 'right to be forgotten' - will be in drafting qualifications to this.

On this point we know that there is considerable sympathy in the UK from the Information Commissioner and UK Government through the Ministry of Justice consultation process with the credit industry's case of this being of critical importance to the lending process.

Consumers exercising this right as drafted would result in fundamentally impacting the data used by lenders through the credit bureaux and also perversely - as the Regulations are meant to help individuals - it would close the door to many looking to obtain a loan.

And we can be confident that arguments like that above - if articulated clearly - should be persuasive at an EU level as in reality the European Council, which in tandem with the European Parliament in the 'co-decision' process, is charged with protecting the economic interests of member states and should appreciate the detrimental impacts of an unqualified 'right to be forgotten'.

The principle requirements of the Regulations have been well-documented in numerous articles and commentary but as ever 'the devil is in the detail' and there is no real substitute for an Article by Article impact assessment.

As a reminder, some of the **'headline' changes** are:

- **Individuals are given stronger and wider rights** including more detailed requirements for subject access; data erasure and correction; a right to be forgotten; and more emphasis being give to 'explicit' consent for processing data.

- A legal requirement for **Privacy by Design** - organisations having to evidence they have thought through new systems and databases against the Regulation's privacy requirements.

- A legal requirement for **Privacy by Default** - currently there is an implied expectation of 'data minimisation' ie only data required should be used. The Regulations envisage the default position as being having to justify *any* data processed and documented decisions being required to support this.

- Mandatory **data breach notification**.

- New **data processor obligations** which will inevitably impact legal, contractual and commercial outsourcing relationships.

- Organisations must develop and maintain **comprehensive documentation**, policies and audit trails to demonstrate compliance with privacy by design and default; document privacy impact assessments, for example around new products and services; and prepare detailed data transfer registers.

- **Data Protection Officers** (internal or an external advisor) will be mandatory for many organisations with a significant expectation around the individual's skills and professional competence.

- **Enforcement** of the Regulations is based on residency. If an organisation transacts - or could potentially transact - with a consumer in an EU member state, then that organisation will be bound by the Regulations.

- Organisations will be accountable to the **supervisory authority** (DPA) in its country of 'main establishment' in the EU rather than in each member state in which they operate - but as there is parallel consistency mechanism to drive DPA co-operation and mutual assistance across member states, there will be significant discussion between supervisors.

  For example, a UK consumer complaining to the ICO about an organisation based in France would necessitate a legal requirement for dialogue between the ICO and the French DPA, the CNIL, to agree the outcome.

WHAT IS THE UK INFORMATION COMMISSIONER'S VIEW?

Christopher Graham, Information Commissioner, speaking at the PDP Annual Data Protection Conference in London on 18th October 2012, said that **"something will happen; the question is when?"**.

His view is that political consensus may be possible by the summer of 2013 and that the European Commission is likely to make some concessions to drive a satisfactory outcome.

While welcoming one of the underlying drivers of the Regulations as being the difficulties experienced by organisations trading cross-border even within the EU due to inconsistencies in the current framework, he did consider that **in their current form the Regulations were over-prescriptive with too much emphasis on process rather than outcome**.

In his view proper accountability of organisations as 'data controllers' should be the dominating factor, and at a supervisory level as written, the Regulations were also over-prescriptive on regulators and would be far too costly to implement.

His office has and is currently responding to the Regulations and researching the true burden on organisations, but the Information Commissioner urged businesses to accept that they have obligations now and these must be addressed.

He highlighted that his office has imposed **£2.5 million fines on 26 organisations** for data breaches over the past 2 years, and based on 60 'best practice audits' there is still clearly room for improvement, especially in local government and the NHS where he is pressing for compulsory rights of audit.

He acknowledged the challenge over an unqualified 'right to be forgotten', especially in the credit sector, and responding to a question from **Regulatory Strategies**, appeared confident that the UK voice would be heard in the lobbying process.

In conclusion the Information Commissioner considered that **the time was right to move on from the 1995 Directive and make data protection changes fit for the 21st century**.

SO IF ALL THIS IS OVER 2 YEARS AWAY, WHY NOT TACKLE THE NEW REQUIREMENTS WHEN WE REALLY KNOW WHAT THEY ARE?

Many organisations, both individually and collectively through professional bodies and trade associations are already trying to shape the Regulations in a way that does not jeopardise their business model - and from personal experience there are some significant concerns.

It is never too early to make issues known both to UK Government (through the Ministry of Justice) and to the European Commission and Parliament.

But underneath the requirements of the Regulations are some sound business processes that should already be embedded in what organisations do with personal data, irrespective of sector.

In the UK, **Privacy Impact Assessments** (PIAs) are not new. Nor is the concept of **Privacy Enhancing Technologies** (PETs), aimed at helping compliant systems' design. But under the new Regulations this type of systematic, documented approach will be mandatory.

So those organisations realising that we are approaching a watershed and that change is inevitable are starting to use these methodologies as a 'best practice' business discipline**. Data protection by design should become a way of doing business today.**

And alongside this organisations are running an internal or external compliance **'health-check'** to ensure their base-point for complying with what the Regulations will impose is at a level that makes migration as seamless as possible and that 'business as usual' can be maintained.

We would urge all organisations irrespective of sector to get to know what's coming. This should be a **strategic Boardroom agenda item** as the Regulations will impact every area of business, both in terms of governance requirements and potential bottom-line impacts.

And make sure the **privacy team -** with the appropriate levels of skill, professional competence and business awareness **-** is in place before the Regulations hit to work on **policies and documentation**.

These are already critical and seen by the Information Commissioner as being essential - and if not in place would certainly exacerbate any data issue in the regulator's eyes and influence the sanctions imposed. Indeed a review of the ICO's enforcement notices and fines shows this all too clearly.

So in simple terms, take action today to prepare for tomorrow. Time spent addressing things now could be the competitive or reputational differential when we open for business on day-1 of the new regulatory regime.

mike.bradford@regulatorystrategies.co.uk

www.regulatorystrategies.co.uk