



# Regulation... Regulation...

## Challenge or opportunity? Tick the 'Data Protection' box now!

Regulatory Strategies ([www.regulatorystrategies.co.uk](http://www.regulatorystrategies.co.uk)) was founded in 2009 on a core 'can do' philosophy, specifically to provide clients with highly practical and commercially focused consultancy around regulatory and consumer affairs. Its culture is to facilitate and enable business, not prevent it.



Mike Bradford  
Director, Regulatory Strategies Ltd.

Over the past three months there have been as many articles about credit industry regulation in the trade press, as more business orientated topics, a sure sign of the times. But while we perhaps run the risk of regulatory overload, it is something we ignore at our peril.

The 'noughties', as the past decade has perhaps ironically come to be known, has been far from plain sailing for the credit industry, with pressures coming from home and the European Commission, putting aside the minor irritation of the global credit crisis.

While comparatively speaking things have been less frenetic for the first part of this year, we are at the crossroads of how the future regulatory framework will shape up with the Department for Business, Innovation and Skills (BIS) undertaking a 'root and branch' review of consumer credit and personal insolvency. The jury is still out on whether this will involve more legislation or self regulation.

At this stage I should put my cards on the table and agree with the comments of Lord Hunt of Wirral, Chair of the Lending Standards Board, that it should not be a choice between statutory or self regulation, they can and should co-exist with the latter underpinning the former in a pragmatic balance. Time will tell.

So perhaps the over arching feeling in the industry in terms of regulation is one of uncertainty, one thing however is a given, there are significant legal, commercial and reputational risks for organisations irrespective of size in today's highly regulated marketplace, in failing to embed core governance disciplines into business practice and corporate culture at all levels, and being perceived by our stakeholders as failing to do so.

At the heart of compliance across all businesses is data protection, and this serves to show the importance of taking regulation seriously at the top of any organisation. Accountability lies in the boardroom, not with the compliance department.

So how sensitive are our customers and the Information Commissioner to data protection in the credit industry?

The Information Commissioner's Annual Report for 2010/11 published in July brings out some critical points for CCTA members and the industry as a whole:

**Lenders again topped the sector attracting most complaints at 13% and organisations found to be in breach are named in the public domain.**

The second most requested publication was 'Credit Explained' at 22,000 copies.

89% of people are aware of their data protection rights, compared to the baseline of 74% in 2004, and an even higher number of young people at 95%, potentially those starting out on their credit journey, are aware of their rights.

The Information Commissioner is targeting increased awareness and consumer education as key objectives for this year.

There is an immediate need to review websites to ensure changes are made to comply with new regulations about cookies, even cookies that do not identify the user and are used, for example, for analytical purpose only.

And the Information Commissioner can now fine up to £500k for breach of the data protection principles, recently extended to cover breaches of the electronic marketing regulations.

I would argue that the facts speak for themselves. Jeopardising consumer trust by being less than responsible with their personal information will go to the heart of our compliance obligations and customer relationships.

Meeting our legal requirements is essential, but with the right approach we can actually build competitive differential and enhance our customer's experience at a time of increasing consumer and regulator concerns and media interest in data protection, privacy and the everpresent fear of a data loss or breach.

If we are not legally compliant, it can lead to action by the Information Commissioner under the Data Protection Act 1998 and Privacy and Electronic Communications Regulations, as well as commercial and reputational damage through being seen by our customers and the market as being irresponsible with personal information.

The Information Commissioner's view (source: The Privacy Dividend: the business case for investing in proactive privacy protection) is that protecting personal privacy makes good business sense.

It should bring real and significant benefits that far outweigh the effort privacy protection requires.

The alternative, of ignoring privacy and leaving personal information inadequately protected, has significant downsides.

Commercial success therefore needs consumer confidence and data protection is really just good business practice for any organisation. It need not stop us doing legitimate and innovative things with data but what it does is to ensure that when doing this we respect the rights of the individuals whose data we are processing.

## The Information Commissioner's Annual Report 2010/11

For full details visit: [http://www.ico.gov.uk/about\\_us/performance/annual\\_reports.aspx](http://www.ico.gov.uk/about_us/performance/annual_reports.aspx)

In addition, the Information Commissioner's Office website reflects on its 2006 "What Price Privacy Now?" report in light of the current phone hacking allegations and the relevance of S55 of the Data Protection Act, whereby it is an offence to "blag" information.

Full details of the consultation on changes to monetary penalties guidance can also be found on the ICO website [www.ico.gov.uk](http://www.ico.gov.uk).

It focuses on the Information Commissioner's Office power to impose monetary penalties of up to £500K which can apply if either an organisation or an individual has seriously contravened the Data Protection Act 1998. Monetary penalties now extend to contravention of the Privacy and Electronic Communications Regulations. The Information Commissioner's Office can also issue an Enforcement Notice for the same contravention.

The Guidance cites examples of serious contraventions. Examples include a disregard for deployment of adequate security measures or an organisation making a large number of automated marketing calls where consent has not been obtained.

The Guidance highlights what would be seen as appropriate measures that an organisation should ordinarily be taking to protect personal data.

In the UK on the whole we enjoy a balanced data protection regime, unlike many of our European neighbours operating under the same Data Protection Directive but where interpretation is far more skewed to privacy per se.

While there are moves afoot to review the Directive and increase harmonisation of approach across EU Member States, we should not jeopardise our position through reckless or careless handling of personal information.

So while we wait to see the future of credit industry regulation, perhaps it is a good time to 'health check' our data protection compliance, as much for business reasons as for regulatory compliance.

**A quick checklist which in itself won't guarantee compliance but will focus on the key areas, would include:**

- who is responsible in our business to ensure we are compliant with the Data Protection Act and that our staff are aware of and trained in our obligations?
- is our register entry with the Information Commissioner's Office accurate and up-to-date? It is a criminal offence not to have this in place.
- is our application form compliant to cover, for example, assessing the credit application, performing a credit search with a credit reference agency, sharing data with other lenders, and additional uses of that data, for example fraud prevention, money laundering checks and debtor tracing?
- what measures do we have in place around data security, including destroying information no longer used?
- do we have a plan in place should any of our customer's information be lost or stolen?

- if we outsource any processing, are these contracts compliant with the Data Protection Act and do we adequately vet our subcontractors?
- is any information processed overseas? What controls do we have in place to ensure compliance with the Act's requirements for transfers outside the European Economic Area (EEA)?
- how do we ensure we keep our customer data accurate and up-to-date, a critical requirement of the Act? Inaccurate data was the second highest number of complaints received by the Information Commissioner's Office in 2010/11 at 15% of the total.
- do all our staff know how to handle a data subject access request? This has a statutory turn around time of 40 days under the Act? In 2010/11 complaints about this ran at 28%, the highest number of complaints raised with the Information Commissioner's Office.
- do we comply with requirements around automated processing and the consumer's right to object to direct marketing?
- is our website compliant in terms of its privacy statement, marketing opt ins/outs, channel preferences and most recently consent for cookies?

Addressing the above would be time well spent and at the very least give peace of mind. Some organisations are increasingly using their approach and commitment to data protection as a competitive differentiator and have publicly signed up to the Information Commissioner's Personal Information Promise.

Data protection is one regulatory challenge, and opportunity, where we can 'tick the box' now.

[www.regulatorystrategies.co.uk](http://www.regulatorystrategies.co.uk)



## Complimentary Seminar Data Protection – a real benefit to your business

Regulatory Strategies is running a complimentary seminar, 'Data Protection – a real benefit to your business' on Friday 7 October at the Belfry Hotel in Nottingham, all CCTA members are welcome.

For full details visit [www.regulatorystrategies.co.uk](http://www.regulatorystrategies.co.uk)

## Banks breaching data rules, says Which? Information Commissioner's Office (ICO) response...

"While the number of upheld complaints is small compared to the millions of bank accounts in the UK, mishandling of financial information can have a serious effect on individuals' lives. It needs to be looked after properly and customer's data protection rights respected. We've identified financial services as one of our priority areas in our draft Information Rights Strategy. We are working closely with this sector to help them make improvements and have been encouraged by their willingness to take action. Of the 515

complaints that were upheld between August 2009 and August 2010, most were linked to customer service issues. This shows that good data protection practices are an important way of building customer satisfaction.

"Consumers who have suffered as a result of a data breach should first exhaust their banks' complaints procedure. They can also seek compensation through the courts. Our Credit Explained guide includes more information on how to do this. Most people only contact

or find out about regulatory bodies when they need to use them, and our services are well signposted both online and by organisations like the Citizens Advice Bureau. Awareness of the ICO among individuals is high, our research puts this currently at 22%, which is a 7% increase since 2005.

"Where we encounter systemic problems, we are committed to taking appropriate regulatory action, including imposing financial penalties in the most serious cases."