

Notes on Workshop F – The Year Ahead: ICO DP Initiatives –

Jonathan Bamford

4 March 2009

ICO Data Protection Strategy

Our strategy sets out our philosophy of how we deal with DP regulation and informs everything we do. Whilst part of our strategy is to minimise DP risk, risk can be a good driver. As the ICO has finite resources we focus on what causes detriment to individuals and society rather than focusing on legal points. Whilst we like to encourage everyone to get it right we do need sticks as well as carrots, and we are pushing for more powers to be able to do this effectively. We are now smarter at maximising our influence, some credit for which has to go to Richard Thomas.

Key Areas for 2009 – 2010

The key areas and how we are going to change the core elements of our strategy:

- Unlawful trade in confidential personal information.
- Public security and surveillance – this has widened from last year, to now include e-borders. Marshalling data centres, passenger details, with all information held in a central database. We are dealing with issues that stem from the ‘surveillance society’, from local authorities using CCTV to investigate school catchment area fraud to the debate as to whether there should be a government data centre for records of our telephone calls.
- Increased information sharing – there are good public policy reasons for information sharing (for example Michael Wills’ malnourished children – that information sharing is necessary to ensure all children who need them get free school meals). The key question is how to do this in a proportionate way. Development of a Code of Practice?
- Privacy By Design – this is new to our strategy, launched at a conference in November.
- Security and integrity of information – integrity is now included – it is not just about security. Information must be of the right quality.

ICO Privacy By Design Initiative

Privacy By Design is all about recognising that increasing amounts of personal information poses increasing risks to individuals. Technology is now so cheap it is easy to retain huge amounts of information but we are lagging behind in ensuring that the information is protected. Data controllers do not always ask the right questions of technology suppliers and data processors.

Technology is not the only solution – Privacy By Design builds in procedures as well as technology to ensure that privacy is built in at the outset. The Data Handling Review and the fact that the Chief Information Officer is now talking the language of privacy impact assessments now is quite groundbreaking.

ID management – there are different forms, based around whether the need is to authenticate or identify. For example a credit card contains just a name but that and



the fact that the credit card company issued a card is enough to authenticate. We are working with BERR regarding ID management.

Privacy enhancing technologies - the Royal Academy of Engineers has commented that no-one asks technologists to come up with new ideas to protect people's information. If they are not asked, they won't do it. Data controllers should consider that even though this can cost a little more it may be worth it. One example of new technology is the 'sticky' privacy policy that ensures information is not used for any purpose it should not be.

Codes of Practice / guidance – the 1998 Act gave the ICO the power to issue codes of practice. The first one was the CCTV Code of Practice, followed by the Employment Practices Code of Practice. We will develop one a year, wherever there is a need.

Information assurance – is about security and quality of information – it is not the same as data protection as DP is also about transparency.

Information governance – we are keen to push this forward. We are working with organisations like the British Computer Society on ways to look after people's personal information as we cannot rely solely on technology to protect it.

Privacy By Design Report

Need to break down existing barriers such as poor privacy awareness at executive levels. We intend to make a difference in the coming year to these.

Delivering Privacy by Design – we need to make the benefits of Privacy by Design clear and ultimately develop a 'Privacy by Design ecosystem'. Privacy impact assessments will help.

Security By Design – Higher levels in organisations are often more comfortable talking about security by design. We need to mainstream Privacy By Design as an organisational issue.

Engaging with executive management - to ensure that executive managers embrace privacy in a holistic way, demanding PIAs in system business cases. Not just a tick box exercise.

One delegate suggested it may be helpful to have a CEO's Rough Guide to Privacy By Design – in a bullet point format which may help buy-in at that level.

Compliance and Regulation

There must be sanctions in place to hold organisations to account for proper processing of personal information. Executive management needs to be accountable, and the ICO needs the power to investigate and enforce compliance where necessary. The ICO is not leading work on the creation of a professional body for privacy practitioners (like a Chartered Institute) but it is an interesting area.

The Personal Information Promise

It is a commitment at a senior level to comply but also to commit resources to looking after personal information – and actually do it! There has even been an early day motion in Parliament applauding those who have signed up and questioning those

who have not. Greater Manchester Police, the Post Office, Unison have signed up. Even Private Eye has asked why no government departments have signed yet.

Organisations are saying it has made a real difference. One organisation changed their data protection processes as they realised they were not adhering to the Act. Another organisation changed their procurement policies.

A look further into the year

- European DP Commissioners' Conference in April – the biggest agenda item here will be how to simplify the EU DP Directive to make it easier to understand.
- We will commission research as to why organisations should spend money on privacy protection, including business cases for Privacy By Design and PETs. This should hopefully encourage vendors / developers to recognise the worth in building privacy into their systems.
- The next Code of Practice should be on privacy and websites.

Privacy Incident Lessons Learned (PILL)

There are lots of incidents that never reach the headlines or the ICO's ears. Data Protection Officers must have a wealth of experience – stories where an issue arose but was sorted out and lessons learned. It would be an online account of privacy near misses.

PILL Key Issues

DPOs would need to get involved. Consideration must be given to what to identify – obviously not the organisation but maybe even the nature of the business might make it too easy to identify the organisation. It may be operated by a 3rd party to maintain confidentiality. Another issue is who should be able to access it – just DPOs or wider access so that anyone can read – this would include, for example, journalists? Authenticity would need to be checked – by some sort of password / restricted access to submit content.

Most delegates suggested they would find it helpful and that they would contribute – and were given a questionnaire to share their thoughts on it.