

Coroners and Justice Bill

Part 8 – Data Protection

Commentary from the Information Commissioner's Office

House of Lords 2nd Reading: 18 May 2009.

Public and political concern about the need to safeguard personal information has never been higher. The power and spread of technology – and the ever-reducing cost of data storage - have been major contributing factors. But concern has also been fuelled by growing awareness of the risks of careless or improper data handling – to individuals and to society. The loss of large amounts of data by HMRC and other public and private organisations has left very few in doubt about the need for strong and effective safeguards.

Data protection has started to be taken more seriously, but this needs to be reflected in modern and effective machinery for ensuring the law works in practice without unnecessary burdens.

The Coroners and Justice Bill provides an important and welcome opportunity to improve the law. The Bill's information-sharing clause has been withdrawn. The other data protection provisions remain. These provisions address some long-standing deficiencies in the Information Commissioner's powers. We welcome the Assessment Notice concept and the statutory data-sharing code.

However, there are **two fundamental weaknesses** in the Assessment Notice procedure (Clause 156) as it stands. We hope that these can be addressed as the Bill makes its way through the House of Lords.

- An Assessment Notice should be available to inspect any data controller, not just those in the public sector;
- There must be a mechanism to deal with situations where a data controller fails to meet a requirement of an Assessment Notice.

We would also like the opportunity to be taken to allow the ICO to serve an Information Notice on those, other than data controllers, who may hold information relating to non-compliance with data protection law.

Assessment notices should be available for all data controllers

An assessment notice will allow the Commissioner to inspect an organisation to check whether it is complying with the data protection principles. At the moment we can only do this with the organisation's agreement. The Commissioner has long since argued that this is unacceptable for effective regulation - a view shared by various Select Committees and others.

Clause 156(3) sets out the types of activity needed for a successful inspection. However, as clause 156 stands, the inspection power will be of limited value because it will only apply to government departments and designated public authorities. This is valuable as far as it goes, but fails to recognise the considerable data risks that can arise outside the public sector. The risks are considerable:

- There is substantial public concern about potential misuse of the internet, and commercial online activity where companies hold enormous repositories of information derived from customers' activities and interests;
- There is growing controversy in particular about targeted (behavioural) advertising and the retention of search engine requests.
- New services, such as Google StreetView, generate new issues.
- Financial institutions hold sensitive records about most adults in the UK, but have a patchy record on security.
- Credit reference agencies can have a significant effect on individuals' lives, helping to determine whether they are given a mortgage or can sign up for a utility.
- Insurance companies increasingly pool customer data. This means that individuals needing insurance have little, or no, control over who has access to their personal details.
- Retailers' loyalty card databases can rival governmental ones in size. They can reveal the most intimate details of shoppers' private lives – their dietary habits, their prescriptions, the films they hire.
- Third sector bodies, often acting on behalf of public authorities, hold large collections of records containing extremely sensitive information about the most vulnerable members of society.
- The ICO recently exposed a secret database holding details of "suspect" workers in the construction industry, which was available to over 40 companies.

Complaints and enquiries received by ICO 2007-8:

Of the 25,946 complaints and enquiries dealt with during financial year 2007/2008, over two-thirds concerned the private sector and under a quarter concerned the public

sector.	
Private:	67.5%
Public:	21.5%
Other (including charities and member associations):	11%

Self-reported data security breaches since Nov. 2007:

Since November 2007 ICO has been notified of 444 breaches. This includes 131 self-reported breaches from the private sector. This figure (approx. 30%) is less than for the public sector, but most public bodies are effectively required by the Data Handling Report to notify breaches. There is no such obligation for the private sector.

High profile data losses have involved major clearing banks, Marks and Spencer, monster.co.uk (recruitment database) and IT contractors to government.

Over several years there has been growing and strong cross-party support for the ICO's assessment powers to be extended to private and third sector bodies.

House of Lords Science and Technology Committee Report on Personal Internet Security, 2006-7

Recommended that the government should examine the *"effectiveness of the ICO in enforcing standards of data protection across the business community."*

Justice Select Committee Report on Protection of Private Data, January 2008

"We hope that this change of heart [the Prime Minister's statement on 21 November 2007 to "do everything in our power to make sure that data are safe"] will lead to powers being provided quickly through legislation." (Para 24)

[NB: This followed a quotation from the Commissioner's evidence about the need to cover all sectors and a reference to the Lords report.]

Thomas / Walport Data Sharing Review (July 2008)

"A large majority of contributors to the review expressed the consistent and strongly held view that the Information Commissioner and his Office (ICO) have neither adequate powers nor sufficient resources to promote or enforce proper information management practices." (7.1)

".....Distinguishing between public, private and voluntary sectors makes little sense..." (7.9)

"The possibility or threat of external scrutiny will do much to encourage organisations in the public, private and voluntary sectors to take compliance seriously. In those cases where there is resistance the power to inspect will need mandatory back-up." (8.61)

Financial Service Authority response to the Thomas / Walport Data Sharing Review, July 2008

"We believe a significant strengthening of the ICO's powers and resources is essential

in ensuring data security, as well as compliance with other aspects of the Data Protection Act, across both the private and public sector.”

House of Lords Select Committee on the Constitution Report, ‘Surveillance: Citizens and the State’, February 2009

“[We] regret the decision not to legislate for a comparable [inspection] power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide.” “[We have] consistently emphasised the increasing role that the private sector plays in our public lives. Services are increasingly contracted out by public authorities as a matter of course. We and other committees of both Houses have consistently noted that private sector data handling and surveillance can impact as adversely on our individual right to respect for private life and the right to respect for our personal information as the same processing in the public sector...”

David Howarth MP (Liberal Democrat), Standing Committee debate

“...holding vast amounts of data is not restricted to the public sector... Purely private organisations have immense power. We should treat them as organisations with that much power when thinking about how they ought to be regulated.”

Henry Bellingham MP (Conservative), Standing Committee debate

“More and more private sector organisations and business are storing our data. The data belongs to taxpayers – our constituents – which is why the Commissioner should have the power to issue assessment notices on private organisations.”

Joint Committee on Human Rights Report, March 2009

“We recommend that the Government reconsiders the Information Commissioner’s request that the proposed power to issue assessment notices be extended to data controllers in the private sector.”

A procedure is needed for non-compliance with an Assessment Notice

The Assessment Notice procedure will allow the Commissioner to serve a data controller with a Notice to enable him to determine whether there is compliance with the Data Protection Principles. The Notice “requires” the data controller to do all or any of the things specified in (a) to (h) of sub-section 156(3). These include permitting entry to specified premises and permitting the inspection of equipment and observation of processing. PWC’s inquiry into the HMRC loss showed how only physical inspection can reveal what is really happening inside an organisation.

It seems very strange, however, that clause 156 of the Bill provides for a right of appeal against an Assessment Notice, but no sanction or other procedure where there is failure to comply. The organisations whose activities are least likely to comply with the data protection principles are the ones that are most likely to refuse an inspection. Clause 156 speaks of “requirements” in an Assessment Notice. But the Commissioner would be powerless when a Notice is ignored or there is otherwise a failure to comply with a so-called requirement. Any regulatory body must be able to take meaningful steps where a statutory requirement is ignored. Otherwise, the Commissioner’s authority and credibility are damaged and the signal is sent that that the law need not be taken seriously.

More specifically, the lack of any sanction matters for two reasons:

- There is no pressure (neither incentive, nor deterrent) for a data controller to comply with a requirement of an Assessment Notice when it is served.
- There is no consequence for a data controller who in fact refuses or fails to comply.

The situation is therefore little improved from section 51(7) of the current Data Protection Act, which only provides for a good practice assessment where the data controller consents.

The nature of the sanction is secondary to the principle. Any approach needs to be effective, to be proportionate and to avoid placing excessive power in the Commissioner’s hands. The Commissioner is very aware that inspection powers can be intrusive and disruptive and fully accepts that a balance must be drawn to ensure no abuses. Paragraphs 8.61 – 8.65 of the Thomas / Walport Data Sharing Review discussed the issues and proposed possible ways forward.

The main options appear to be:

- Criminal offence for a data controller who fails to comply with a valid Assessment Notice requirement (modelled on section 47 of the Data Protection Act which provides for failure to comply with an Information or Enforcement Notice served by the Commissioner.)
- Contempt of Court (the sanction for non-compliance with a Decision by the Commissioner under the Freedom of Information Act).

