The Data Sharing Review — raising the spectre of tougher enforcement in the UK

Bridget Treacy, Partner at Hunton & Williams, ***analyses the content of the recently published Data Sharing Review, and examines the new enforcement proposals which are set to transform the nature of data protection compliance in the UK***

Bridget Treacy is chairing the 7th Annual Data Protection Compliance Conference in London.

For more information on this Conference, which takes place on the 2nd and 3rd October 2008, please visit www.pdpconferences.com

The last nine months have marked an extraordinary period for data protection enforcement in the UK. In the immediate aftermath of the discovery of now infamous HMRC data loss, there was extraordinary public outrage at the cavalier fashion in which HMRC had shared personal information, and a sense of disbelief that the Information Commissioner ('Commissioner') possessed only rudimentary enforcement powers with which to respond to the breach.

Attention has increasingly focused on the amount of data sharing taking place within both the public and private sectors. Advances in technology have made data sharing easy, but have also promoted a more collaborative style of working. Frequently collaboration is on an informal basis, extending across organisations. Within the public sector, the government has pursued an e-government strategy, resulting in increased data sharing. Within the private sector, the pressure to respond quickly to, and even anticipate, consumer demand, has led to sophisticated data mining and consumer profiling. All of these activities have been supported by technology which enables vast quantities of data to be collected, used, stored and shared — all quickly, cheaply and often without much thought.

The Data Sharing Review ('Review'), commissioned by the UK government just prior to the HMRC data breach in October 2007, and published on 11th July 2008, contains radical proposals for strengthening the enforcement powers of the Commissioner. The Review, together with the subsequent immediate steps taken by the government detailed below, suggest that more proactive enforcement of the Data Protection Act 1998 ('DPA') is inevitable.

The terms of reference

Dr Mark Walport and Richard Thomas led the Review into how personal information is shared in the public and private sectors. Their terms of reference were to:

- consider whether there should be any changes to the way the DPA operates in the UK and the options for implementing any such changes; and
- provide recommendations on the powers and sanctions available to the Commissioner and the courts in legislation governing data sharing and data protection; and
- provide recommendations on how an organisations' data sharing policy should be developed in a way that ensures proper transparency, scrutiny and accountability.

The authors concluded that changes are necessary in five key areas:

(i) the transformation of organisations' culture insofar as how they influence the way personal data is collected and used;

(ii) the legal framework governing data sharing;

(iii) the effectiveness of the Information Commissioner's Office ('ICO') which oversees data sharing;

(iv) the existing mechanisms that enable research and statistical analysis for the public benefit, whilst safeguarding the privacy of individuals; and

(v) the safeguarding of personal information held in publicly available sources.

Specific recommendations were made in relation to each of the areas. This article focuses on the first three of the five numbered above.

Initial considerations —should personal data be shared?

Within the public sector in the UK, there has been a growing focus on how data sharing may be facilitated, but less focus on how data are collected and whether data should, in fact, be shared at all. The process of collecting data will often determine whether and, if so, to what extent data may be shared. Many organisations simply assume that they are entitled to

(Continued on page 8)

(Continued from page 7)
share the personal data that they hold. Consumers generally resent this.

In this context, the Review notes that peoples' attitudes to data sharing are influenced by the degree to which they feel that they have real choice and a degree of control over the collection and use of their data. These factors are frequently overlooked by organisations, yet public trust and confidence are strengthened by clear identification of who is responsible for handling the data and who is accountable for it. The Review urges organisations to focus on the question of whether data sharing is appropriate in the particular context and, as part of this assessment, to consider five factors: proportionality; consent; legal ambiguity; guidance; and people/training. While there is no single test for determining when it will be appropriate to share personal data, the Review encourages organisations to think carefully, in each case, about why it is necessary to share data and what impact the data sharing may have on privacy. Undertaking a structured privacy impact assessment can help an organisation to anticipate and deal with any privacy issues.

The Review also acknowledges that there is no generally held consensus as to the degree of choice and/or control which an individual should be able to exercise in relation to the sharing of their personal information. Where possible, people should be asked to consent to sharing but this will not always be practical, meaningful or appropriate (i.e. in the context of law enforcement). The issue of consent needs to be considered in context. Consent will be most relevant in a 'provision of services', rather than a 'public protection and law enforcement' context. In the former, real choices can be made, although the Review does provide the caution that where consent is used, it must be transparent and understandable. Particular criticism is made of consent which is false or uninformed, i.e. standard terms which offer no real choice to an individual.

"rather than simply indicate that data will be shared with 'selected third parties', organisations should publish a list of the third parties with whom they share data"

How should data be shared?

It was the manner in which HMRC shared data, rather than the decision to share the data, which was the focus of the many criticisms made of HMRC in the Poynter Report (see *Privacy & Data Protection Journal, Volume 8, Issue 7, pages 7— 8).* Staff at HMRC relied on the fact that data had been shared before, without examining the specific facts. Further, there were multiple points of contact within HMRC which led to inconsistency, security was a low priority, 'surplus' data were not redacted, and the data sharing was not formally authorised. These failings were fatal. In contrast, the Review encourages organisations to consider the following four factors when considering how to share data:

- **Leadership, accountability and culture:** there must be senior leadership responsibility for personal data. Unlike the US environment, responsibility for data protection in the UK is too often given to a junior member of staff. Responsible handling of personal data must be part of an organisation's culture, and requires the visible support of senior leadership.
- **Transparency:** people must be informed about the purposes for which their data will be processed. Usually a 'fair processing' statement or privacy notice serves this purpose, but frequently these notices are vague, complicated and too long. Notices should be clear, people should be able to access the data which is held about them, and people should be told that data are processed by third parties. The Review goes as far as to suggest that rather than simply indicating that data will be shared with 'selected third parties', organisations should publish a list of the third parties with whom they share data.
- **Technology:** the Review encourages organisations to use technology to enhance data security alongside acknowledging that the power of technology may also serve to increase the risk of data being compromised. The Review deliberately steps away from adopting a prescriptive approach to possible technical solutions.
- **Cultural barriers to sharing:** the Review notes that confusion and misunderstanding appear to be the main barriers to data sharing.

Enforcing the DPA — powers and resources of the regulator

One of the most significant sections of the Review is the discussion of the Commissioner's powers and resources. These powers are widely regarded as inadequate and insufficient. There is a common perception that data protection enforcement in the UK lacks teeth. Consequently, there is a widespread perception that if an organisation breaches the DPA, they will escape sanction. This perception looks set to be challenged.

The recently enacted Criminal Justice & Immigration Act 2008 ('CJIA') amended the DPA to give the Commissioner the power to impose substantial fines on an organisation which breaches the Data Protection Principles deliberately or recklessly in a manner likely to cause substantial damage or distress. The Review recommends that the fines imposed by the Commissioner should mirror those which may be imposed by the Financial Services Authority ('FSA'), and that the powers should be brought fully into effect by 8th November 2008.

The Review also makes the case for creating a 'realistic threat' of regulatory inspections, spot checks or audits to incentivise organisations to take their obligations seriously. (At present, the Commissioner requires the consent of an organisation before an inspection or audit may be undertaken.) Further, the Review contains the recommendation that the notification fees, which fund

the ICO's caseload, should be increased from £35 per annum.

Key recommendations in the Review —

1. Cultural changes

According to the Review, organisations handling significant amounts of data should indicate in their corporate governance arrangements where ownership and accountability lie for personal information. Organisations should also review their internal controls over data on an annual basis, report to their shareholders (if relevant), and promote transparency by:

- ensuring privacy notices are drafted in plain English and prominently displayed;
- ensuring privacy notices state what data are held, why, how data are used, who can access data, with whom data are shared, and for how long data are retained;
- publishing a list of organisations with which or to which they share, exchange, or sell personal information;
- using clear language when asking people to consent to sharing data;
- enabling people to inspect, correct and update their information; and
- reviewing and enhancing staff training on handling personal information.

2. Legal framework

The UK government should, says the Review, assume a leadership role in promoting reform of EU data law. Provision should be made for a statutory fast track procedure to remove or modify existing legal barriers to data sharing, including a requirement to obtain an opinion from the Commissioner as to the compatibility of the proposed sharing with data protection requirements.

The Commissioner should also have a statutory duty to publish a data sharing code of practice.

3. Regulatory body

In addition to calls for the CJIA to be fully in force by 8th November 2008, and the proposals that fines mirroring those imposed by the FSA, the Review recommends that organisations notify the Commissioner of significant data breaches. Further, where substantial damage or distress is likely, the Review states that the Commissioner should be able to take into account any failure to notify when setting any penalty for breach. The Commissioner should also have statutory powers to enter premises to carry out an inspection.

The Review states that annual registration fees for data controllers should be increased, adopting a tiered approach based on the size of the organisation.

Finally, the Review calls for the regulatory body to be reconstituted as a multi member Information Commission, rather than a sole Commissioner.

Next steps — inspection powers and funding

Just ten days after the Review was published, the Ministry of Justice responded by publishing a consultation paper on two of the key recommendations contained in the Review: the proposal for the Commissioner to have increased inspection powers, and the proposal to review funding arrangements.

In its consultation paper, the government has proposed that data controllers should have the option, when they register with the Commissioner, to consent to a good practice assessment ('GPA'). If the controller then suffers a serious data breach, the fact of prior consent to a GPA will exempt it from being fined pursuant to the new section 55A DPA. (There is no protection in respect of criminal offences.) Controllers may withdraw their consent to a GPA on giving three months notice. Further, the government would enhance the Commissioner's powers to enable him to specify the time and place for the provision of information pursuant to an Information Notice. Currently the Commissioner can set a deadline in an Information Notice by which information must be provided, but he cannot specify the manner in which this is done. According to the proposals, the Commissioner would also be able to demand, during an onsite inspection, information to enable him to determine whether the controller is complying with the DPA. The Commissioner's existing powers do not currently extend this far.

The government is considering allowing the Commissioner to apply for a warrant where he does not have reasonable grounds to suspect a breach of the DPA, but where he has identified the organisation as high risk. The Commissioner would be required to explain to the court why he needed the warrant. This proposal is narrower in scope than that recommended by the Review with the government apparently concerned by the prospect of the Commissioner having the power to enter premises with a warrant and then to undertake a random audit.

In relation to funding, the government proposes a tiered notification fee structure, and a new sanction for controllers who knowingly or recklessly provide incorrect information as part of their registration.

The views of data controllers on the proposals were sought as part of the government's consultation, which closes on 27th August 2008. The inspection proposals are particularly likely to attract significant comment.

Conclusion

The data protection landscape in the UK has transformed during the last twelve months. This period of transition will be ongoing, with the implementation of the proposals contained in the Review. The fact that the government has taken immediate steps to implement key recommendations expanding the Commissioner's right to audit and increasing his funding, sends a clear message that data protection is being taken more seriously in the UK.

Bridget Treacy
Hunton & Williams
btreacy@hunton.com