



**Information Commissioner's Office**  
Promoting public access to official information  
and protecting your personal information

## **Taking stock, taking action**

# **The ICO position on the Government Data Handling Reviews**

## **Contents**

Introduction and background	3
Information governance	5
Policy and procedure	7
Transparency	9
Technology	11
Training and awareness	12
Culture change	14
Implementation	16
Other issues	17
Summary of ICO actions	22



## Introduction and background

At the end of June 2008, a series of reports were published on the handling of personal information.

- The review of information security at Her Majesty's Revenue and Customs (HMRC).
- The Independent Police Complaints Commission (IPCC) independent investigation report into the loss of data relating to Child Benefit.
- The report into the loss of Ministry of Defence (MOD) personal data.
- The review of data handling procedures in Government.

These were followed by the publication of the Data Sharing Review on 11 July 2008. The publication of these reports represents the culmination of the unprecedented examination of information sharing and data protection issues that has occurred over the last twelve months.

In light of the importance of the issues that have been raised in the various reports, the Information Commissioner considers it appropriate to put on record his position on some of their recommendations, and provide some further information on action the ICO intends to take as a result of their findings.

In his speech on *Liberty* on 25 October 2007 the Prime Minister stressed the importance of public trust in the sharing and use of personal information. In light of this he announced that he had asked Mr Richard Thomas, the Information Commissioner, and Dr Mark Walport of the Wellcome Trust, to undertake an independent review of data sharing across the public and private sectors, examining whether there should be any changes to the way the Data Protection Act 1998 operates and options for implementing such changes (the Data Sharing Review).

In November 2007, Her Majesty's Revenue and Customs (HMRC) lost the personal details of over 25 million citizens. Information included in the loss included the names of parents and their children, their addresses and the bank account details of child benefit claimants. In response to this loss, the Prime Minister set up a review of data handling procedures in Government (the Data Handling Review), to be led by Sir Gus O'Donnell, Cabinet Office, to work with Departments and security experts to examine and improve data handling in Government.

At the same time the Chancellor of the Exchequer commissioned Kieran Poynter, the Chairman of PricewaterhouseCoopers, to conduct an investigation into the loss of personal data at HMRC, as well as conducting a root and branch review of processes and systems as they relate to handling at HMRC. The Independent Police Complaints Commission, having jurisdiction by virtue of the Police Act 2002, also initiated its own investigation into the series of events leading up to the loss of data at HMRC in order to ascertain whether any criminal conduct or disciplinary offences had been committed by HMRC staff.

On 9 January 2008, a Royal Navy laptop computer containing unencrypted records for more than 600,000 people was stolen. The Secretary of State for Defence commissioned Sir Edmund Burton to conduct a review to establish the exact circumstances and events that led to the loss by MOD of personal data; to examine the adequacy of the steps taken to prevent any recurrence, and of MOD policy,

practice and management arrangements in respect of the protection of personal data more generally.

Four of the reports were published on 25 June 2008, with the Data Sharing Review published on 11 July 2008. Between them, the reviews have made over one hundred recommendations, ranging from specific recommendations on management structures and accountability within Government Departments to general recommendations on improving the operation of data protection law.

## Information governance

*“The fact that no senior official was involved in the events leading to the data loss raises serious questions of governance and accountability.”* (Review of Security at HM Revenue and Customs)

*“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”* (the seventh data protection principle)

All five reports identified shortfalls in corporate accountability and the governance of information. One key theme which comes out of all five reports is that information governance is not being adequately addressed at executive level within organisations, and, as such, information risks and liabilities are not being recognised or addressed.

Various executive and management structures have been suggested, with a number of different roles and actions at senior executive level recommended. The reports differ slightly in how these actions, roles and structures work in practice, but there are a number of common themes.

- A role should be created at board level in larger organisations to deal specifically with information risk.
- A post at senior executive level should oversee information security.
- Information security and risk management should become part of wider security and risk assessment programmes within the organisation management structure.
- Periodic reporting of information risk and governance issues should take place at board level.
- Organisations should set in place an information risk policy.
- Identification of information held, what is added, what is removed and who has access to that information, both within the organisation and third parties.
- Clear lines of accountability should exist in the management of information, with “ownership” of certain information assets or flows being introduced across the organisation.
- These lines of accountability should ensure that people, as well as processes and technologies, are managed as part of the information governance structures.
- Effective formalised programmes of information assurance and audit should be introduced, using third parties where necessary to ensure the independence of these functions.
- IT procurement procedures should adequately reflect information risks.
- Where a contractor provides information management services, there should be an agreement between the relevant parties which details responsibilities and reflects the policies of the contracting organisation.
- A working principle should be adopted of collecting, using and disclosing the minimum amount of personal data.
- Information about governance arrangements should be detailed in annual reports and added to the organisation’s statement of internal controls and thus be subject to audit.

The ICO welcomes these themes. Not only do they make for sound business practice in the management of information assets, they also go a long way to ensuring compliance with the seventh and other data protection principles. Sound information governance structures are vital to ensure that the protection of personal information is given proper attention at all levels of the organisation. While the reports focussed on the handling of personal information in large government departments, the common themes that they present are undoubtedly relevant to other large organisations. The thinking behind these themes, if not all the detail presented in the reports, should be considered by any organisation that processes large amounts of personal information or personal information of a particularly private or sensitive nature. Sound information governance should take account of governance of the process, technology and people in an organisation.

The ICO has always been clear in recognising the benefits of sensible sharing of personal information. However, we have been equally consistent in calling for appropriate protection to be put in place at all levels within an organisation that shares personal information. The benefits of this are that other parties, such as the recipients of personal information, the individual and the customer, can all continue to reap the benefits of sharing personal information without confidence and trust being shaken by high profile data losses. While we recognise that much work has been done in improving information governance over the last year and are realistic in recognising that one can never completely eliminate the risk of data loss, the fact that the ICO continues to receive significant numbers of notifications of information losses indicates that both the public and private sector have to continue to improve in this area.

## Policy and procedure

*“Government has put in place a core set of mandatory minimum measures to protect personal information, to apply across central Government. They are minimum measures in that they oblige individual Departments and agencies to assess their own risk, and those organisations will often put in place a higher level of protection” (Cross Government Actions: Mandatory Minimum Measures)*

*“However we are not seeking compliance with the law as an end in itself. Making our vision a reality means minimising data protection risk for individuals and society. The law is the main tool we have at our disposal to achieve this, but we go further and promote good practice. Good practice may go beyond simply meeting the requirements of UK law but will always be consistent with the law as well as with the EU Data Protection Directive (95/46/EC) and ultimately with the right to respect for private life enshrined in Article 8 of the European Convention on Human Rights”. (A Data Protection Strategy for the Information Commissioner’s Office)*

Policy and procedure for protecting personal information do not exist in isolation. The policies have to be accessible and useful for employees to ensure that they are fit for purpose and can be implemented effectively. Several reports highlighted that policy and procedure were quite often in place, but was rarely read and used appropriately by the majority of staff. This was down different factors, such as documents running to many hundreds of pages or specific policy documents have a limited circulation among staff.

The ICO welcomes recommendations to simplify, shorten and make guidance more accessible across organisations, with structured hierarchies of guidance from short briefing documents for all staff to in-depth technical guidance for specialists. It is also useful to see recommendations that general policy guidance should be translated in locally applicable procedures in each organisation and in some cases, in each line of business within an organisation.

In particular, the ICO welcomes recommendations to introduce specific measures, such as:

- more proactive incident management;
- clearer and more robust storage, retention and deletion policies;
- internal data handling and sharing procedures;
- definitive external disclosure and sharing procedures;
- clearly defined roles and responsibilities when information is shared, both within an organisation and externally;
- policies for use and disclosure of personal information based on need; and
- regular review and updating of information policy to ensure that it remains fit for purpose.

The ICO welcomes the development of a new protective marking for personal information in Central Government. The “PROTECT – PERSONAL DATA” marking, with the related guidelines for handling such information, will provide clear and easy to follow procedures when using, storing and disclosing the personal data. It will also ensure that personal information which falls within the definition of the protected

marking will be treated with the same degree of sensitivity as other “PROTECT” marked information across government. The level of protection required for this information is spelt out in direct and understandable terms in the Cabinet Office’s document Cross Government Actions: Mandatory Minimum Measures. Other personal information will still be considered “personal data” and will require a basic level of security and protection in order to meet the requirements of the Data Protection Act 1998.

One of the key recommendations that appeared across the various reports was greater use of Privacy Impact Assessment (PIA). PIA is a process by which the privacy risks inherent in the use, sharing or disclosure of personal information can be addressed at the design stage of a project and solutions found. Issues such as proportionality and necessity can be adequately addressed during the PIA process and this can inform decision making in relation to the use of personal information. A PIA is a transparent, consultative process which relies not only on robust internal analysis of risks and liabilities from an information assurance perspective, but also on wider privacy concerns raised by stakeholders such as the citizen, private sector partners or other bodies and agencies to whom information is disclosed or from whom it is received.

In December 2007, the ICO launched the PIA Handbook. This is the first handbook for PIA in the UK and has generated a lot of interest from the public and private sectors. The ICO is aware of a number of PIAs already underway and the interim report on Data Handling Procedures in Government mandated the use of PIA in Central Government. The ICO sees greater use of PIA as a means to ensure that more thought is put into using personal information at an early stage of a project rather than data protection compliance being considered at the final stages before a project is launched. The ICO has published the PIA handbook in order to provide a clear structure for completing PIAs and will be complementing the handbook with a short supplementary user guide which will be developed over the coming months.

PIA should be seen as part of information risk management within an organisation and sits nicely alongside other disciplines such as information assurance and security management. While welcoming the recommendation to mandate the use of PIAs within Central Government, the ICO would echo the recommendations in other reports for much wider use of PIA across the public and private sectors and will be continuing to help build the business case for this.

The ICO would also echo the recommendation that the decision making process in relation to sharing personal information should be better documented, with details about the business case for sharing personal information, the risks and benefits, the necessity and the proportionality detailed in an appropriate manner. This could be done as part of the PIA process and would not only lead to better decision making but also to transparency.

## Transparency

*“Only when people better understand what happens to their personal information will they invest more trust in the organisations that process it. And only when levels of trust are suitably high will organisations be able to take full advantage of the potential benefits offered by the use of personal information, passing on those benefits to the public through more efficient, better-value services.”* (Data Sharing Review)

*“Personal data shall be processed fairly.....”* (first data protection principle)

Transparency in the actions of organisations that use and share personal information is not just a matter of compliance with the law – it is vital for public trust and confidence. The Data Protection Act 1998 sets out the information which must be provided to individuals as part of the requirement to process information “fairly”. This legal requirement for transparency was underpinned by the introduction of the Freedom of Information Act 2000, the aim of which was to change the culture of the public sector from “need to know” to “right to know”. By now, 10 years after the introduction of the Data Protection Act 1998, most organisations that use personal information should have in place “fair processing notices” to inform individuals who they are, what information they hold, the purposes for which they hold it and any other information required to make the processing “fair”.

Likewise the introduction of publication schemes under the Freedom of Information Act 2000 has set out a requirement on the public sector to publish certain information proactively in order to raise public awareness. The mechanisms for providing information to the public about what an organisation uses personal information for and who the organisation might share such information with should already be in place.

The ICO nevertheless welcomes the recommendation for greater transparency across all five reports, in particular the recommendations for:

- publication of “information charters” by all Government Departments, setting out standards people can expect from public bodies that request or hold their personal data and what they can do if they think the standards are not being met;
- publication of material about specific information assets;
- publication by Cabinet Office of the new requirements on Government Departments;
- clearer use of terms such as replacing “fair processing notice” with “privacy policy”; and
- greater prominence being given to fair processing notices on an organisation’s printed and online literature;
- more effective and better use of privacy policies, including layered policies;
- clearer information on who is receiving information and what protections are in place, including details about which organisations personal information is sold to;
- ensuring individuals are provided with the information they require to assert their rights to access and correct information and that the mechanisms for doing this are clear and accessible.

These recommendations should not be an additional burden on organisations, as they mainly bring an organisation up to the level of compliance with the law. Some of the recommendations do require an organisation to go further than mere compliance, but they ought not to be onerous, particularly when seen in light of the need to build trust and confidence in their handling of personal information.

The ICO supports the idea that people should be provided with a full picture of what their personal information will be used for at the time it is collected. When an individual has a choice as to whether they provide their information or not, that decision must be underpinned with the necessary information so that the individual can provide genuine, informed consent. Where the individual has no choice, it is equally important that they understand the process and purposes for which their information will be used, what the limitations on the use of their information are and what they can do if something goes wrong.

On the topic of consent, it is important that organisations are clear to the individual when genuine, informed consent is a condition for using their information. It is also important that, where an organisation seeks to rely on genuine consent that they make it clear how consent can be withdrawn and what happens where this occurs. As stated in our submission to the Data Sharing Review, where an organisation wishes to keep an individual informed and does this by asking for their consent, consent becomes a false notion if the information is shared regardless of whether the individual refuses. Such an approach devalues the concept of consent and makes the process of collecting, using and sharing personal information more opaque to the individual.

If the public and private sectors wish to engage individuals, they must ensure that the process, purposes and the terms under which personal information is collected are clear and transparent.

## Technology

*“The pace of technological change is quickening. The level and sophistication of external threats, such as e-crime, is increasing.”* (Data Handling Procedures in Government: final report)

*“Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—*

*(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*

*(b) the nature of the data to be protected.”* (DPA interpretation of the seventh principle)

Technology is constantly changing and the means and methods that we use today to protect information may be obsolete by tomorrow. Use of security technologies should always be proportionate to the nature of the information being protected. However, better use of technology alone will not be enough to make the transfer or use of personal information secure. For this reason the ICO welcomes the recommendation that the use of technology should be underpinned by clear and accessible guidance and policy on its use.

The ICO supports recommendations on making personal information accessible through secure links to central servers, as this is generally a more secure way to transfer information than through removable media. Transfers should only occur on the basis that satisfactory arrangements are in place for storage of the transferred information, and the system for transfer itself is both secure and has adequate recovery processes in place should it be compromised.

The ICO also welcomes recommendations to:

- audit the use of all removable media devices;
- make access control consistent across all systems;
- ensure that all non-laptop removable media are formally approved and accounted for on a regular basis;
- to adopt appropriate technological solutions in accordance with the seventh data protection principle;
- ensure that the technology supports audit trails of the use of personal information and the secure but easy interrogation and monitoring of these audit trails;
- issue clear guidance to staff on the use of private mobile devices to process an organisation’s information assets;
- examine the practicality of limited use of privately owned personal computers for limited organisational tasks; and
- offer free, safe disposal for technology which is used to process personal data.

The implementation of these recommendations should not be seen as a one off exercise. The use of technology and the policy that informs it will need to be routinely reviewed to ensure that it remains fit for purpose.

## Training and awareness

*“The officials involved in this matter had received little or no information security training since their induction into the organisation”* (Review of Information Security at HM Revenue and Customs)

*“The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.”* (DPA interpretation of the seventh data protection principle)

One issue that all five reports have recognised as vital to the protection of personal information is staff training and awareness. Policies may be in place, procedures may be developed, but if staff are not aware of the legal obligations of the organisation when handling personal information, or how the organisation intends to meet those obligations, then the potential for information security to be compromised remains high.

The ICO welcomes recommendations that take a strategic approach to staff training and awareness, in particular recommendations to:

- closely align training, human resources and communications functions within organisations to ensure that process and procedures are embedded in staff behaviours;
- ensure that staff at all levels understand their responsibilities and apply their learning in day-to-day activities;
- ensure senior staff are regularly briefed on information security risks and vulnerabilities;
- provide regular refresher training to staff;
- ensure that training and awareness are seen in the context of the life cycle of employment, not merely as part of an induction process or a one-off training event;
- make poor information handling a competency or disciplinary issue;
- treat information security as a key staff competency
- develop clear, brief guidance that is easily accessible to staff;
- provide shorter, more accessible versions of policies and procedures to staff;
- make staff aware of risks and vulnerabilities specific to the processes they are undertaking and provide training to mitigate and avoid these;
- make staff aware of the key information assets they use and the records and audit trails that must be kept; and
- provide specific training on the Data Protection Act 1998.

The importance of staff training cannot be overstated in increasing information security. As the *Data Sharing Review* reported, most breaches of information security occur as a result of human error. Effective staff training and awareness of information security and wider data protection issues will not only address the risks of breaches, but also equip staff to be better able to identify risks and vulnerabilities themselves and escalate concerns where necessary.

However, the recommendations go further that simply addressing the need for general staff training and awareness across the organisation, they also stress the need for senior staff to be regularly briefed on information risk and vulnerabilities. The aim of these recommendations is also clear, that it is not simply training for the sake of

training staff, but to ensure that behaviours at all levels of staff are adapted to meet the information security and data protection needs of the organisation and the individuals whose personal information is being held. It is important that staff in the public and private sectors do not view access to and use of personal data as a right, but as a key asset with which they have been entrusted.

## Culture change

*“The highly sensitive nature of the data held on the two CDs was, surprisingly, appreciated by only a few members of HMRC staff. Even though those who had concerns did voice them, no attempt was made to clarify the position relating to authority levels and physical protection of the data during transfer.”* (IPCC independent investigation report into the loss of data relating to Child Benefit)

*“.....information sharing is often viewed as an innate good in itself, rather than a useful tool for achieving legitimate aims. This has at times hampered debate about the risks inherent in an increase in collection and sharing of personal information. As a result, the potential exists for information sharing operations to go ahead without sufficient consideration of the risks involved and then without the accompanying safeguards to mitigate those risks.”* (ICO response to the consultation by the Data Sharing Review)

The ICO welcomes the recommendations in areas such as information governance, training and awareness and transparency. Implementing these measures will contribute in themselves to changing the culture and attitudes within organisations. They will help both by ensuring that information sharing is not seen as a “magic bullet” to the extent that risks and vulnerabilities are left unrecognised and unaddressed and also by ensuring that personal information is seen as a valuable and sensitive asset and, more importantly, is treated as such.

The ICO nevertheless welcomes and echoes the recommendations which point to the need for a wider cultural shift in relation to attitudes towards collecting, holding, sharing and disclosing personal data. In particular the ICO welcomes:

- a working principle of collecting the minimum amount of personal data;
- more thorough examination of the reasoning and necessity for collecting personal information;
- greater consideration of using authentication rather than identification of individuals as part of service delivery; and
- organisations viewing good data protection as underpinning the benefits of information sharing, rather than as an obstacle.

In particular, the ICO welcomes the fact that the recommendations generally do not focus exclusively on the need for culture change among staff generally, but also recognises the need for leadership from senior management. This is essential in ensuring that the entire organisation appreciates the sensitive nature of the personal information it processes and the need for effective data protection to be put in place.

The need for culture change is strong. Since the reports were published there have been more examples of personal information being treated in an almost cavalier way. Part of this culture change can be adopting the information charter, but this needs to be accompanied by a meaningful commitment by senior management to data protection. And this commitment needs to permeate not just the culture of the organisation, but the culture of contractors and consultants with whom personal data is shared.

One key element of this is the matter of budgets allocated to projects which involve some form of processing of personal information. Providing adequate protection for this information will not always require additional money, but budgets must reflect the unavoidable costs of privacy protection in new projects. These elements of the budget must not be the first to be cut when finances are stretched.

Organisations must also be aware, and make sure that their staff are aware, that responsibility for ensuring adequate levels of protection of personal information are not abdicated once such information is passed to a third party contractor or partner. It is the responsibility of the organisation that passes such data on to ensure that suitable protections are in place and that, where a data processor is being used, that suitable instruction is provided as to how the information should be treated. Where it is appropriate to encrypt personal information, this should not be avoided because of expense, inconvenience or because the organisation considers that once the personal information is passed on it is no longer their responsibility. Such attitudes fail to recognise an organisation's full range of responsibilities as data controller under the Data Protection Act 1998 and present practical dangers of personal information loss.

## Implementation

*“A culture of formal, rigorous Information Risk management and security of personal data has yet to be embedded across the Defence community. The recent losses, though highly regrettable, have at least highlighted this important issue.”* (Report into the Loss of MOD Personal Data)

*“It is of fundamental importance that lessons are learned from these breaches”.*  
(Richard Thomas. Information Commissioner, 25 June 2008)

The investigations into the losses of personal information at HMRC and the MoD highlighted that both organisations had in place policies and procedures which, if followed, might have avoided the losses and have mitigated the potential for misuse of the personal information lost. While the recommendations contained in the various reports are welcome, this is only the beginning of the process of implementation of new policies and procedures. The publication of the various investigations and reviews should not mark the end of the period of activity and change which was initiated in October 2007. The challenge now is for every organisation, across the public and private sectors, to embed the policies, procedures, accountability and culture changes in day to day practice.

The ICO issued enforcement notices to the MOD and HMRC on 14 July 2008. These enforcement notices add statutory force to the recommendations in the reports by Sir Edmund Burton, the IPCC and Kieran Poynter. The enforcement notices require that ICO receives reports at three, six and twelve months on the progress HMRC and MOD have made in implementing the recommendations.

Some recommendations have provided specific direction for organisations to consult with the ICO on the compliance of certain databases and practices with data protection law. The ICO welcomes these recommendations and is always open to being consulted on these issues.

The ICO welcomes the publication of a timetable for implementation of the core measures to protect personal information in Central Government. The ICO is itself subject to these recommendations and will be implementing the recommendations of the Review of Data Handling Procedures in Government.

An important aspect of implementation will be how the organisation is seen to enforce new guidelines, security measures, policies and procedures. The ICO welcomes recommendations for management to be rigorous in enforcement of security instructions and policy and for failure to adhere to stated policies and procedures to be treated as a disciplinary offence. However, failures in information security and data protection should not be seen as purely a staff problem. Many of the findings across the reports point to a failure at the most senior level of management to provide leadership and the policies and procedures provided to staff must be fit for purpose.

## Other issues

*“We believe that changes to the law are also required, not least because they should help to embed the necessary new attitudes to personal information within organisations’ hearts and minds.”* (Data Sharing Review)

*“An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.”* (long title of the Data Protection Act 1998)

In addition to the common themes that appeared in all five of the data loss reports, there were a number of issues raised as part of the Data Sharing Review which relate directly to the work of the ICO.

### 1. Review and reform of the EU Directive 95/46/EC

The ICO has recently awarded a contract to RAND Europe to conduct a review of EU data protection law. The purpose of this review is to stimulate debate about the strengths and weaknesses of the EU Data Protection Directive (95/46/EC). This recognises the pace of technological change, the pressures on privacy and integrity of personal information and ever-increasing public awareness and concerns about the need for effective safeguards. It also reflects a growing feeling that the Directive is becoming increasingly outdated, is not sufficiently clear in its objectives, is more bureaucratic and burdensome than it needs to be and is out of step with good regulatory practice.

This work will result in a report which will be discussed at the Spring Conference of European Data protection Commissioners, which the ICO is hosting in Edinburgh in April 2009, and published later in 2009.

### 2. Statutory Code of Practice on data sharing

In October 2007, the ICO published the *Framework Code of Practice for Sharing Personal Information*. This was not a statutory Code of Practice but was developed in light of the Information Commissioner’s general duty to promote good practice under section 51 of the Data Protection Act 1998. The Framework Code of Practice has been widely welcomed.

The Ministry of Justice is considering whether separate legislation should be introduced requiring the Information Commissioner to publish a statutory code of practice on sharing personal information and update the code as required. The current *Framework code* will provide a basis for any statutory code the ICO may be required to produce.

### 3. Sanctions under the Data Protection Act

The Commissioner’s new power (s.55A DPA) to impose financial penalties on organisations found to be deliberately or recklessly breaching the data protection principles was created by the Criminal Justice and Immigration Act 2008. A number of

the provisions of section 55A in relation to the extent of monetary fines and the procedural rights of organisations are reliant on the introduction of regulations by the Secretary of State.

The ICO has been in discussions with the Ministry of Justice in relation to the exercise of the new power to impose financial penalties and we hope that the necessary regulations will be laid before Parliament later in the year.

#### 4. Inspection and audit powers of the regulator

Section 51(7) of the Data Protection Act 1998 currently provides the Information Commissioner with the power to assess any processing of personal data for the following of good practice. However, this power can only be exercised with the consent of the organisation the ICO wishes to audit.

During his speech on Liberty the Prime Minister provided an undertaking that the ICO would be able to conduct spot checks on Government Departments in order to assess their compliance with data protection law. The ICO has been making the general case for greater audit and inspection powers for a number of years now and would like to see this power set on a statutory footing and expanded to include the entire public and private sectors. The ICO has already undertaken a review of its data protection operations with a view to increasing capacity to undertake spot checks on Central Government and expects the first of these to be completed by the end of 2008.

The ICO published the paper *Data protection powers and penalties – the case for amending the Data Protection Act 1998* earlier in 2008. This paper called for, among other powers, the power to inspect personal data and the circumstances surrounding its processing without the consent of the organisation concerned. The Ministry of Justice has consulted on increasing the Information Commissioner's powers and the ICO is waiting for its proposals.

#### 5. Breach notification

We note the fact that none of the reports recommended that notification to the Information Commissioner of information security breaches should be set on a statutory basis. Since the HMRC loss of personal information, the ICO has had voluntary notification of over 270 information security breaches from other organisations on a "confessional" basis. As part of this the ICO has developed some guidelines for organisations on when a security breach should be notified and what information about the breach needs to be provided to the ICO. This has been working well in practice.

The ICO can see the potential benefit of some limited form of formal, statutory notification of information security breaches, whether to the individuals affected, the ICO or both. This has been introduced in a number of jurisdictions around the world, most notably in the USA. In some cases, it appears to have been successful as a driver for encouraging good practice. In others, an initial glut of public breach notifications has led to "breach fatigue". We have doubts as to whether it would be possible to frame legislation that strikes the right balance. It is therefore important that before any new legislation is brought forward that the practicality and long term effect

of such a requirement is fully explored. We also agree with the findings of the *Data Sharing Review*, which states a failure to notify security breaches should be a factor which is taken into account should a monetary penalty be considered under section 55A of the Data Protection Act 1998.

It is worth noting that breach notification is being considered as part of the review of Directive 2002/58/EC (the EU Directive on privacy and electronic communications).

## 6. Resources of the regulator

The budget for regulation under the Data Protection Act 1998 comes from notification fee income which currently stands at around £10.5 million. This is our total budget for advising data controllers and the general public, investigating complaints, developing policy and guidance, conducting data protection audits, taking prosecutions and operating the register of notifications. In addition, this budget has to pay the majority of the costs of the ICO support functions such as human resources, communications and external relations and IT services. This is a very small budget in comparison with other regulatory bodies, particularly considering that there are over 300,000 data controllers on our register.

In the light of these budgetary constraints, taking on significant new regulatory tasks, as well as maintaining our existing roles in the face of increasing demand, will present real difficulties. We therefore welcome the suggestion of introducing a tiered fee regime for notification. A two or three tiered fee regime would reflect more fairly the cost to the ICO as regulator of differently sized organisations, and address the perceived unfairness of businesses that process information about just a few people paying the same fee as large companies or government departments that process information about millions of people.

This issue is also being addressed as part of the Ministry of Justice consultation on the powers and funding of the ICO.

## 7. Constitution of the regulator

One recommendation that needs further consideration is to change the single commissioner model under the current legislation to an alternative model in which the regulatory body is re-constituted as a multi-member Information Commission. In particular, the Data Handling Review was of the firm opinion that the current single commissioner model is not best placed to lead and manage the ICO in the future.

The advantages of a multi-commissioner model are laid out in the Data Handling Review and the ICO accepts that there are some strong arguments for adopting a multi-commissioner model. The current Information Commissioner, Richard Thomas, introduced a new structure involving the establishment of a Management Board for the ICO which goes some way towards replicating the multi-commissioner model. However, further significant changes in the model cannot occur without a change in the law.

## 8. Overcoming legal obstacles and the absence of powers

The Information Commissioner has always been of the opinion that the Data Protection Act 1998 is no barrier to legitimate, proportionate, well thought out information sharing programmes which have appropriate protections built in. However, we do recognise that often there is sometimes confusion over whether an organisation has the statutory powers to share information or is prevented from sharing information due to a statutory prohibition.

The ICO welcomes the proposal to provide for a closely defined power by order to remove barriers to information sharing in specific cases. It is important that where this is available it is subject to necessary safeguards and controls and the Data Protection Act 1998 clearly applies. The proposal is explicit in stating that the power should be provided in primary legislation, which would allow for debate in Parliament and would require the Information Commissioner to issue an opinion on the compatibility of the proposed information sharing. This would be informed by a PIA.

This proposal will need careful thought to be translated into a workable process. The PIA would need to be started when any new information sharing project is being designed and the Information Commissioner would have to be able to issue his opinion at an early enough stage in the process so that any problems he identifies can be addressed. The ICO is already in discussions with the Ministry of Justice as to how this proposal might be taken forward.

## 9. Research and statistical analysis

The use of personal information for research purposes has often raised complex questions. Practitioners across a range of research disciplines have to ensure that any use of personal information is compliant not just with data protection law, but with other regimes that regulate their area of research, such as the law of confidence or professional standards.

While compliance with data protection law is facilitated by an exemption under the Data Protection Act 1998, the complexity and demands of relevant standards and other legal requirements mean that researchers find it difficult to clarify the ground rules and ensure compliance.

The ICO agrees that the creation of 'safe havens' for research would clear up some of the confusion surrounding the use of personal information for research purposes. However, to be effective, the safe havens must ensure the highest standards of security and protection for personal information, particularly where this information is of a sensitive nature. Researchers who wish to make use of the personal information in safe havens should be subject to some form of accreditation and there should be appropriate penalties for anyone who misuses or abuses the personal information provided in the safe haven. In addition, personal information should be provided on the basis of need for each piece of research, with use of anonymisation and pseudonymisation where this is suitable. The creation of safe havens for research might require legislative change. The ICO is happy to provide advice on how this might work in relation to data protection law should the Government decide to move forward with this idea.

## 10. The sale of the edited electoral register

The Data Sharing Review recommended that the Government removes the provision allowing the sale of the edited electoral register. The edited register would therefore no longer serve any purpose and so would cease to exist. The ICO understands the thinking behind the Data Sharing Review's recommendations and would not be opposed to a move in this direction. However, the ICO has previously accepted the current arrangement of allowing the individual to opt-out of the edited register as being in line with the provisions of data protection and other relevant legislation. The ICO has no plans to promote any further action in relation to the sale of the electoral register.

## Summary of ICO action

- The ICO is reviewing its own information governance in the light of the core measures for protecting personal data recommended in the Cabinet Office report.
- The ICO has responded to the Ministry of Justice's consultation on 'The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998'.
- The ICO has issued enforcement notices to both the MOD and HMRC which require both organisations to take steps to ensure compliance with the third and seventh data protection principles. The steps include implementing the recommendations from the Review of information security at Her Majesty's Revenue and Customs and the IPCC investigation (for HMRC) and the report into the loss of Ministry of Defence personal data (for MOD). Both MOD and HMRC are required to report on their progress in this area periodically over the coming year.
- The ICO is developing its "personal information promise", a series of commitments to handling personal information that are made at board level in an organisation and are publicly available. The aim is to demonstrate senior level commitment to DP and by doing so drive up compliance and public confidence in the use of their personal information.
- The ICO is continuing to make the guidance and advice we issue as clear, accessible and consistent as possible. This includes:
  - reviewing and launching a suite of core guidance on the Data Protection Act 1998;
  - guidance on managing data breaches;
  - continuing to promote the use of Privacy Impact Assessments, updating our handbook in light of experience.
  - producing our code of practice on privacy notices this coming year to provide organisations with some clear good practice guidance on collecting personal information in a transparent and clear way;
  - continuing to promote the use of the Framework Code of Practice on Sharing Personal Information.
- The ICO is leading a 'Privacy by Design' programme to:
  - encourage public authorities and private organisations to ensure that as information systems which hold personal information and accompanying procedures are developed, privacy concerns are identified and addressed from first principles;
  - encourage organisations to design privacy and data protection compliance into systems rather than ignoring it or bolting it on as an inadequate afterthought;

As part of this work, the ICO has asked the Enterprise Privacy Group (EPG) management team to support the initial research and produce a report on the topic. This report will form the centrepiece of the ICO's Privacy by Design conference on 26 November 2008.

- The ICO is continuing to support staff with data protection responsibilities through the annual Data Protection Officer's conference, to educate and influence

stakeholders, and will continue to promote the need for good information governance generally.

- The ICO continues to raise awareness within organisations of their obligations and encourage good practice within organisations.