CabinetOffice

Data Handling Procedures in Government: Interim Progress Report

Making
government
work better

Introduction

1. On 21 November, the Prime Minister announced that he had asked the Cabinet Secretary, with the advice of security experts, to work with Departments to ensure that all Departments and all agencies check their procedures for the storage and use of data.

2. The terms of reference for the work are to examine:

- the procedures in Departments and agencies for the protection of data;
- their consistency with current Government-wide policies and standards;
- the arrangements for ensuring that procedures are being fully and properly implemented;

and to make recommendations on improvements that should be made.

3. The work is proceeding in parallel with, but will be informed by, the separate work being conducted:

- by Kieran Poynter of PricewaterhouseCoopers into the specific circumstances in HM Revenue and Customs that surrounded the loss of personal data; and
- the work commissioned in October from Richard Thomas (the Information Commissioner) and Mark Walport of the Wellcome Trust to look at the security of personal data in both the public and private sector.

4. All Government Departments and agencies are currently involved in an intensive process of examining and improving where necessary their data handling arrangements. The scope of the review covers UK government Departments only, but the devolved administrations are being kept informed of work as it progresses. Given that data are often shared across boundaries, all the relevant administrations recognise the importance of working together on this issue, although it is for each to reach decisions on the detail of their own arrangements.

5. This document provides a brief update on progress of the work in advance of a final report expected in Spring 2008. It summarises the work that has taken place to date across Government.

6. This work will continue, with particular focus on arrangements in place in arms-length bodies and contractors, transfer of data on removable media, safe disposal of classified waste, and with a programme to tighten procedures for any data stored outside the UK. Work will cover both the safe management of data within given Departments as well as data sharing, including with statutory regulators and scrutiny bodies.

Protection of data by Government

7. There are close links between the action needed to protect personal information in Government and day to day management of the business of public service, and Departments are best placed to understand the nature and sensitivity of the particular information they hold. As a result, responsibility for ensuring that the necessary arrangements to protect data are in place must always primarily rest with individual Departments. Government must ensure that Departments exercise that responsibility within an appropriate legal and administrative framework, and support them in doing so, while recognising the differences in the challenges that they face.

8. New approaches to delivery of public services and new technology present new challenges in ensuring the right protection for information. Some of the ways in which Government as a whole has adapted the legal and administrative framework include:

- enacting the Data Protection Act 1998 (DPA), updating previous legislation and implementing the 1995 European Directive on Data Protection. The DPA requires anybody processing personal information to comply with eight principles, one of which is to ensure that personal information is secure;

- requiring, in February 2004, all Departments to appoint a Senior Information Risk Owner (SIRO) as accountable for the ownership of information risks within that Department;

- building information assurance into the Office of Government Commerce Gateway process, which examines programmes and projects at key decision points in their lifecycle; and

- most recently, announcing the power for the Information Commissioner to conduct "spot checks" on Departments to provide additional external scrutiny.

9. In 2003, the Government established in the Cabinet Office the Central Sponsor for Information Assurance (CSIA). CSIA is responsible for providing strategic direction in information assurance across Government, guided by a National Strategy for Information Assurance. Under this Strategy, refreshed in 2007, CSIA provides guidance to Departments in the management of information.

10. The Government constantly develops guidance to support Departments and agencies and keep up with changes in technologies. Advice on the management of information risks is available from the British Standards Institute in the ISO 27000 family of standards for information security management systems. These were developed in close co-operation with experts in the Cabinet Office and CESG, the part of GCHQ that acts as the National Technical Authority for Information Assurance, to address the full range of information security policy and good practice. They are reflected in a set of information security standards developed for Government, and incorporated in the Government's Manual of Protective Security. This was first issued in 1994, and has been regularly refreshed since then.

11. The National Information Assurance Strategy provides a framework for considerable activity, including:

- long-term research and capability development programmes involving CSIA, CESG and industry to increase technical capacity and greater availability of information assurance solutions to support the safe sharing of sensitive data across Government;

- the inclusion of information assurance in the Office of Government Commerce's new framework contracts and in the Chief Information

Officer (CIO) Council's enterprise architecture design for future government ICT;

- improving awareness of information risk management within Government through better training and deepening the professionalism of information assurance experts;

- work by CESG and the Centre for the Protection of the National Infrastructure (CPNI) to improve assurance processes and update guidance to meet new threats to Government and the wider national infrastructure; and

- Get Safe Online[1], a joint public and private sector initiative to raise awareness of internet safety for the general public and small businesses.

12. Under the DPA, the Information Commissioner has a general duty to promote good practice by data controllers and in particular to promote the observance of the requirements of the Act by data controllers. In fulfilment of this, the Information Commissioner's Office (ICO) has published a series of guides designed to make data protection simpler, targeted at organisations and individuals alike.

Update on progress

13. The work to date has primarily focused on examining arrangements in place for storage and use of data within the existing framework. Heads of Department have been asked to ensure that arrangements applied meet the policies and standards laid down centrally, and that there are robust procedures to ensure that they are followed properly.

14. The focus in these early stages has been on policy and procedure, but has involved Departments identifying specific instances of potential data compromise. As part of good practice, Departments should routinely notify the Information Commissioner of any significant instances of potential data loss and this process will continue as the work progresses. The Information Commissioner has indicated that on the basis of the information he has

[1] http://www.getsafeonline.org/

received so far, none of the instances appear to present a substantial risk to large numbers of individuals.

15. As set out above, within the overall framework for information assurance, responsibility for ensuring that the necessary procedures and operations to protect data are in place must always primarily rest with individual Departments. All Departments have taken action to remind staff of their responsibilities as regards data handling. Departments have also instigated work to check internal compliance with policies and standards, with particular focus on the transfer of data on removable media and the safe disposal of classified waste.

16. Individual Departments face different challenges according to the nature and sensitivity of the data that they hold and its volume. Following the initial work, all are taking specific actions tailored to their circumstances. The material below summarises some of the actions being taken in Departments.

17. The Cabinet Office is reviewing its internal security policies in light of the recent HM Revenue and Customs (HMRC) data loss. Departmental data copying is already audited by an automated software product and further enhancements to encryption procedures are underway.

18. The Crown Prosecution Service has over 600 sites attached to its network. It is re-examining a small number of areas, including access to portable media, the encryption of backup tapes and the arrangements for local back-ups to ensure that current arrangements are secure.

19. The Department for Business, Enterprise and Regulatory Reform is reassessing its risks associated with data sharing. Staff have been reminded of existing policies and procedures, ensuring that the interdependency between information management and security is well understood and the links tightened. BERR is also engaged in work with its arms-length bodies to ensure that these policies and procedures are understood and applied.

20. The Department for Children, Schools and Families has reminded all staff about their data and information security responsibilities. It has commissioned an independent review of the current and proposed information security arrangements for the ContactPoint project – a key element of the

project to transform and combine information on children's services. An initial positive report has been given, with the main report due for completion in January 2008.

21. The Department for Communities and Local Government has a knowledge management strategy that seeks to embed recognition amongst staff that data are valuable resources that must be protected with proper procedures in place for their management. All major system owners are instructing their contractors and partners of the need for high standards of data management. This is being extended to arms-length bodies.

22. The Department for Culture, Media and Sport works with a wide range of organisations including 2012 Olympic delivery partners. DCMS's information management strategy is under review, as part of a long term business transformation programme. Guidance has recently been produced for arms-length bodies on information assurance and further guidance is being considered on information management. In addition, specific work on information flows and management across the 2012 delivery partners has been commissioned, with recommendations due by the end of January 2008.

23. The Department for Environment, Food and Rural Affairs is carrying out a review of compliance with information assurance procedures. Its delivery bodies are also being asked to review their procedures and implement any necessary improvements.

24. The Department for Health is already undertaking a major review of NHS information systems to cover the Department, the NHS and all arms-length bodies. Following the Medical Training Applications Service breach the Department has signed an undertaking with the Information Commissioner to improve departmental policies. Subject to Parliamentary approval of the Health Bill, a National Information Governance Board with statutory authority will be established. Following the HMRC data loss, all staff have been reminded of security procedures and discussions with internal audit are underway to conduct a review of personal data handling within the Department.

25. The Department of Innovation, Universities and Skills is a recently formed Department and has adopted procedures from its predecessor

Departments. It has commissioned an independent review in support of its data handling procedures. An action plan will be instigated upon receipt of the review.

26. Whilst the Department for International Development does not hold large amounts of personal data relating to members of the public, it does hold significant volumes of commercial and security data. It takes a risk-based approach to information security and is reviewing its decisions on the controls over the storage, retrieval and transmission of all sensitive data.

27. The Department for Transport has been reviewing its data security and is tightening data management as a result. Measures include accelerating plans to transfer data electronically, wherever this is reasonably practicable and cost effective, merging databases to avoid the need to transfer data between locations and regular reporting on information management. In addition the Permanent Secretary has written to senior officials in the Department – including Agency Chief Executives – drawing their attention to current guidance on the application of the DPA.

28. The Department for Work and Pensions, which deals with large numbers of citizens, has, following the HMRC data loss, put in place a temporary ban on physical transfer of data on removable media. Refreshed guidance is being produced for staff to inform them when secure services must be used to transfer personal data. A secure same day courier service has been developed. The same day provision is a robust full track-and-trace courier service with dedicated drivers from collection to delivery points. DWP have established a task force and a senior executive to oversee the work.

29. The Foreign and Commonwealth Office has previously made substantial investment to ensure it adheres to information security standards, and is working closely with CESG in the accreditation and monitoring of its systems. The FCO is due to issue reinforced instructions to UKVisas staff on data protection issues and will issue additional DPA guidance to all staff to emphasise and advise on the practical implications of the Act's security requirement. The FCO will use the information collected for this review as the basis for regular oversight of the handling of its major accumulations of personal data.

30. The Home Office published a corporate strategy on information in February as part of its Reform Programme for public protection started in July 2006. This is being reviewed in the light of recent events. An independent review commissioned prior to the HMRC data loss will report early in the New Year and any issues raised will be addressed. Since the HMRC data loss, the Home Office Senior Information Risk Owner (SIRO) and Chief Information Officer (CIO) have briefed all Directors on their responsibilities, as well as tasking network Security Compliance Officers to reinforce key messages on data and protective security measures.

31. HM Revenue and Customs has taken a number of steps to strengthen its data security arrangements since the recent data loss. It is co-operating fully with the external reviews, including the review by Kieran Poynter, and other investigations looking at the specifics of the incident, as well as wider data security issues. Recommendations emanating from these studies are likely to cover security management standards and data handling. Specific actions already taken include the appointment of a senior official, Director of Data Security, and the appointment of Data Guardians to all areas within HMRC. Key principles for data handling and security have been revised in a new set of operating standards and guidance for all staff. Improvements and controls have been put in place regarding removable media and its transfer – including restrictions on personal computers to prevent download to removable media. Longer term strategic solutions to data security are being discussed, including the use of electronic data transfers, which would lead to a reduced usage of removable media. HM Treasury is enhancing its own staff education and training in security backed by senior management leadership and increased emphasis on compliance.

32. The Ministry of Defence has reassessed its policies and procedures in light of the incident with HMRC data, and is taking forward work to ensure that bulk data transfers are better protected and will make more explicit the need for early involvement of Data Protection Act specialists. MoD is seeking to achieve the same consistency in assessing the sensitivity of non-operational data in terms of impact level and classification as it routinely does with operational and research-based systems.

33. The Ministry of Justice is a new organisation, and is rolling out new policies and procedures. Work includes reviewing the means by which

guidance is disseminated and made available to staff, the overall corporate governance arrangements for information management, training provisions, and arrangements for bulk data transfer and outsourcing. The Ministry of Justice is aiming to complete this work by April 2008. In addition, subject to the outcomes of the wider Government review, the Ministry of Justice will undertake an audit of data protection compliance by April 2008.

34. The Northern Ireland Office is developing governance provisions to emphasise further senior management's ownership of information assurance, and undertaking a review of policy and procedure documents. Relevant training provisions are also under examination in order to increase understanding of these issues across the Department. The NIO board is focusing on the enhancement of governance arrangements and on direct accountability to the board for risk management and information assurance. This work will relate both to NIO and its arms-length bodies.

Next steps

35. Work on the specifics of data handling arrangements, some of which has been described above, will continue. As noted above, there is a wide range of activity taking place within Departments, including with delivery bodies reporting to them, as well as the general work to focus on the transfer of data on removable media and the safe disposal of classified waste. A programme will be put in place to tighten procedures for any data stored outside the UK. Work will cover both the safe management of data within given Departments as well as data sharing, including with statutory regulators and scrutiny bodies.

36. In parallel, the work will examine the overall framework within which Departments manage information.

37. Even the most sophisticated systems for data handling – including best practice in the private sector – will never be entirely risk-free. Government holds a huge variety and amount of information on citizens and businesses. Some Departments maintain a wide range of information systems themselves, each holding a significant number of records. To deliver public services effectively and efficiently, information needs to be shared between different parts of Government.

38. Equally, the public have a right to expect the information that they provide to Government will be held securely and used appropriately. The Government's ability to deliver and improve public services relies on high levels of public trust. Government has always regarded personal data of citizens as a critical asset akin to the most sensitive financial and other information handled within Departments. This should continue to be Government's underlying principle. The challenge is to ensure that information is collected, used, and, where appropriate, shared, effectively and securely.

39. Given the nature of the systems and processes involved, as well as future changes in technology and services, work on information assurance will always be an ongoing process. In common with the private sector, the challenge will remain one of risk management and constant improvement, within an overall approach of managing information to support service delivery.

40. Further work around the framework within which Departments can operate and how they can be best supported in doing so will include consideration of:

- governance, accountability and leadership within Departments, including best practice in ensuring a professional approach to information risk management;

- the relationship between information assurance and work on information sharing as part of Transformational Government, to ensure that arrangements are sufficiently strong and flexible to accommodate improvements in public services and technology;

- approaches to information policies, standards and risk, and in particular how Departments can be best supported through guidance; and

- enforcement and compliance, including the right nature and level of external scrutiny.

41. Some initial recommendations in these areas can however be made on

the basis of the work to date, which are set out below.

42. It is clear that more can be done to improve trust and confidence about the arrangements in place to protect information in Government. Transparency should be a powerful tool in this respect. As a first step, Government should commit to enhanced transparency with Parliament and the public about action to safeguard information and the results of that action. Departments should cover information assurance issues in their annual reports. Ministers should present to Parliament an annual report on the issue as a whole.

43. As set out above, the responsibility for ensuring that the necessary arrangements to protect data are in place must always primarily rest with individual Departments. There is more that can be done to ensure that this primary line of accountability works as well as it could do. Government should revise guidance to Departmental Accounting Officers, to ensure that their annual Statements of Internal Control explicitly include the systematic coverage of information assurance. Systematic notification of this material and any significant incidents during the year to the Cabinet Office and the Information Commissioner should ensure that emerging cross-cutting themes and lessons are identified and shared as necessary.

44. Legislative steps should be taken to enhance the ability of the Information Commissioner to provide external scrutiny of arrangements. The Government has already announced the powers to permit “spot checks” on central Government Departments, and should commit to extending this to the entire public sector, and consult early in the New Year on how this can best be achieved and funded. The review commissioned in October from Richard Thomas (the Information Commissioner) and Mark Walport of the Wellcome Trust will look at the issues around personal data in both the public and private sectors. The Government should consult quickly with those potentially affected on how the relevant recommendations can best be achieved.

45. Similarly, the Government should commit in principle to the introduction of new sanctions under the Data Protection Act for the most serious breaches of its principles. Such proposals will have to take account of the need not only to provide high levels of data security, but also ensure that sensible data sharing practices can be conducted in an environment of legal certainty.

These proposals should be covered in the same consultation process.

46. Government should build on the steps already taken, to continue to develop the mechanisms by which Departments are supported in the exercise of their responsibilities towards data security. Government-wide guidance to those involved in data handling, setting clear common standards and procedures for Departments on data security, should be further reviewed, focusing on the support provided to those performing particular roles, such as the Senior Information Risk Officer. Given the importance of data to improving public service delivery and in tackling crime including fraud, such guidance should not only cover questions of security, but also a requirement on the owners of significant public sector information assets to consider how they can best be used to support the delivery of public services or to help to tackle crime, consistent with high levels of data protection and legal provisions.

47. A further report will be made in Spring 2008.

CABINET OFFICE
DECEMBER 2007