

NLAWARP White Paper Number 3

Data Handling

Introduction

Three reports have been published recently about Data Handling in the Government and Public Sector space. They are:

- ◆ Data Handling Procedures in Government: Final Report, which was undertaken by the Cabinet Office;
- ◆ Sir Edmund Burton's Report into the Loss of MOD Personal Data for the Permanent Under Secretary Ministry of Defence;
- ◆ and the Review of information security at HM Revenue and Customs: Final Report, by Kieran Poynter.

Each reportⁱ makes a different set of recommendations that will impact widely on the public sector, the third party organisations that work with the public sector, and the wider business community.

However, it is not only Her Majesty's Government (HMG), but also large commercial organisations, that have had well documented instances of breaches of confidentiality of personally identifiable data.

HMG has rigorous controls in place to securely manage departmental data – protective levels are assigned that rank data into impact levels one through to six. Yet for citizen's data, such precautions do not appear to be in place. To date there have been few guidelines as to how and when citizen's data is managed, with respect to internal access and availability, as well as to where, and with whom, that data is shared.

While the Cabinet Office report makes recommendations to redress this situation it also clearly states that each government department is responsible for assessing and managing its own data handling requirements, and that where appropriate individual departments may go beyond the minimum recommendations to secure information.

All of the reports accept that personal data must be stored and is required in order to provide better and more personalised services. However, data should be properly safeguarded as the Government is a custodian rather than the owner of the data. Indeed a new concept of 'protected personal information' has been introduced. Another common theme is that end users, ie staff, must be given clear guidance on the treatment and handling of data, including regular training, and that data security measures must be quantifiable, transparent, and easily open to scrutiny.

Government departments clearly need to rebuild their reputation for taking care of personal data by following Data Privacy measures and ensuring that staff are educated and motivated to view personal data as a highly important, valuable and sensitive commodity.

So how do organisations go about complying with three different sets of Data Handling recommendations? How do you ensure that staff understand and adhere to data security policies, and how can you prove that policies are followed? On top of this, with the ever increasing drive to push down costs, provide more flexible working for staff, and share data with third parties to provide better services, how can you implement stronger data security systems?

This white paper examines various recommendations and discusses 'real-world' solutions that are CESG CAPS approved where they need to be, that provide secure yet flexible working options, and that do not impact on business performance. In other instances products are to be CCTM approved.

The Reports

Data Handling Procedures in Government: Final Report

In his forward Sir Gus O'Donnell says:

'Effective use of information is absolutely central to the challenges facing the Government today – whether in improving health, tackling child poverty, or protecting the public from crime and terrorism. Those in public service need to keep that information secure, in order to build public confidence. This is essential to underpin greater data sharing to deliver personalised services and make us more effective.'

Sir Gus goes on to say:

'No organisation handling information can guarantee it will never experience losses. But people have a right to expect that their public services achieve and maintain high standards in this important area. Those involved in delivering those public services must work harder and be more effective to meet and exceed those expectations. Every loss or near miss must make us more determined. The action now underway will raise our game, but the task of improving information security will always be a continuing process.'

A significant recommendation from Sir Gus's report is the introduction of mandatory minimum security measures across Government when handling personal data, which includes encryption.

The report introduced the new concept of 'protected personal information', which is personal information that merits protection. The report also introduces the idea that the Government is the custodian of personal data and does not have the right to regard it as the Government's own information.

'Protected personal information' is defined as:

- ◆ Identifiable personal information where disclosure would lead to significant risk or distress
- ◆ Any database of over 1000 records of personally identifiable information

A new way of dealing with this information is recommended which includes:

- ◆ A set of security and management measures to ensure consistent protection
- ◆ A change in attitudes which will be fostered by training
- ◆ Accountability for the information in the possession of the department
- ◆ Transparency and scrutiny of department data handling.

Cabinet Office recommendations for the core measures to protect information

The report comments that while Departments are already provided with plenty of security policy advice, guidance and information, a new shorter set of core minimum requirements should be applied across the board.

Departments may go further than the minimum but this is the common level that they must meet. The recommendations relating to the transfer of data include:

- ◆ Specifying that personal data benefits from higher levels of protection
- ◆ Where possible, not transferring such information, but accessing it on its home system or remotely via a secure channel
- ◆ Where transfer must occur, doing this through secure electronic transfer, so that discs are phased out where possible
- ◆ Where data has to be put onto removable media such as discs or laptops, minimising the information transferred and using encryption
- ◆ Putting in place new controls to limit user rights to transfer data to removable media such as discs and to check the use of those rights

Poynter report on Information Security at HMRC

Kieran Poynter, chairman of PricewaterhouseCoopers was commissioned by HM Treasury to write this report. He makes 45 recommendations, all of which have been accepted by Chancellor Alistair Darling, and concludes that better implementation and enforcement of policy is required, and that policy could be made more accessible and be better communicated.

Within the report Mr Poynter proposes ten principles for information security in the electronic age. While these are specifically targeted at the HMRC, they equally could apply to any organisation.

1. Data about an entity (be it an individual or a business) belongs to that entity. It can be entrusted to other parties but always remains the property of the entity to which it refers
2. It follows that it is the responsibility of the entity to maintain its own data
3. Data becomes information when it has value. This typically happens through context and through aggregation. The ambition should be never to lose or allow undesired access to information. Key to this is segregation – ie. separating out data when it is stored and designing jobs and the systems that support them to require a minimum of information
4. HMRC should hold the minimum data required to perform its functions, including the retention period it holds data for. It should not, for instance hold data that it can get elsewhere but it should routinely make use of other sources of data that improves its ability to tailor its service to its customers
5. HMRC should hold data about entities once – it should move to a single customer record for individuals and a single customer record for businesses
6. Effective information security requires both service provider and customer to play their part. HMRC should have the powers to be able to specify secure methods of exchanging data with its customers, starting with businesses and over time including individuals
7. HMRC should have regard to external sources of guidance on information security such as Data Protection legislation and the guidance given to the financial services sector by the FSA

Information security measures should be focused on the area of biggest risk, data transfer. It follows that:

8. Transfers of digital data involving physical media should be phased out completely
9. Paper-based communications should be rationalised as to content and frequency with a long term plan of substantially eliminating them
10. Computers (and in the short term, any removable media) should be encrypted so that if they are lost or stolen any data or information on them cannot be accessed

An additional recommendation particularly worthy of note is that the HMRC should enhance its business continuity management.

Report into the Loss of MOD Personal Data

This report was penned by Sir Edmund Burton for the Permanent Under Secretary Ministry of Defence. In the report Sir Edmund makes 44 recommendations, all of which have been accepted.

The recommendations that directly affect data sharing and handling include: Recommendation 25: That the Department supports initiatives making personal data accessible through secure links to central servers, on the basis

that clear guidelines are in place for onward storage of this data, and the system itself is both secure and has adequate redundancy

Recommendation 26: MOD to produce clear policy on sharing personal data with third parties, including changes to standard contractual clauses as required.

Recommendation 27: To instigate a full census of non-laptop removable media device holdings, in order to ensure that they are formally approved and accounted for on a routine basis

Recommendation 28: MOD to implement guidelines on the storage of personal data on these devices, including the requirement for encryption, as necessary

Recommendation 29: MOD to reiterate, or revise, Departmental guidance on the use of private mobile media devices to process MOD data

Recommendation 36: MOD to consider adopting appropriate technological solutions to achieve compliance with data protection regulations

Recommendation 43: Urgent consideration to be given to procuring a simple, affordable solution to enable the safe, authorised, use of personal (privately owned) computers for limited Government tasks, on an individually licensed basis.

What does this mean?

All of the reports call for a change in culture to one where personal data is treated with upmost respect. This will happen slowly through the re-education of staff to understand the implications of safe data handling procedures. Yet, how do you impose another set of policies on an already beleaguered workforce?

The key is have computer systems that underpin set policies and procedures, with which people will comply, by either controlling or monitoring behaviour. This can be achieved by implementing data security systems that are transparent to the end users so that it has no impact on the way that they work, and that are centrally managed so procedures can be monitored and enforced, with audit trails to prove compliance and highlight any irregularities.

The issues of data management

As the reports note, there are challenges to managing data. Not just the questions of how and where it is stored, but how much data is required and for how long? As the reports suggest, there is no need to store more data than is really required and for longer than is necessary, nor should it be sent to places where it isn't required.

The issues of data aggregation and lifecycle management require policies in place. Not only is a policy required, but the procedures for compliance and auditing the policy adherence. A third area of vulnerability for data is who is accessing the data, and what specifically they have access to. For an organisation this means policies in place to monitor the 'back-end' – where the data is stored – and access by the end user at the front end.

Sharing information securely

Security and confidentiality breaches of protected personal information indicate that Government departments need to develop policies and procedures to handle citizens' data more sensitively - particularly when sharing information with third parties which is seen as the biggest risk area.

It is important to enable shared services, so data should be protected in such a way that it is still easy to access for authorised recipients. Information that leaves direct control needs to have clear processes in place to protect it and ensure that the right person is authorised to receive and access it. These issues have driven a number of initiatives, including the New Assurance Model coming from CESG, that have resulted in new products that allow the secure export of data, as well as the control of the data by the authorised recipient.

Although the aim is to phase out the use of removable media for the transfer of data or sharing it with third parties, in the short term many departments will still need to use this method. To solve this problem there are now Government approved products available that provide a 'zero footprint' encryption option, where data files have built in encryption that protects the data, without making it difficult to access because the decryption of the information is automatic when the authorised recipient authenticates. In addition these solutions can define how data is handled once received at the destination. There are also controls and an audit trail to track what information has been sent, what is received and ensure that it is not tampered with in transit.

Better yet, is for data to be accessed on its home server so that the data never actually leaves its safe protected environment. This can be achieved by rolling out a cost effective solution that gives secure access via a virtual private network.

This is ideal for staff that need to work away from secured headquarters, maybe from a third party's premises, or while out on the road doing their job or from home. Alternatively it can be used to grant other organisations access to data without the overhead of having to set up permanent network access. Users are issued with a USB device that carries a secure, encrypted operating system that enables them to boot from any machine and access defined areas and files on the network.

The device is totally isolated from the host machine so there is no possibility of cross contamination of viruses and other malware or data leakage. If lost the USB device is totally encrypted so no data can be assessed.

With the deployment of such solutions, citizens and employees can be assured that the integrity and confidentiality of their personally identifiable data is appropriately managed.

A previous white paper in this series outlined Socitm's top 10 tips for Data Handling, these are still very valid. The Local Government Association (LGA), in conjunction with Socitm and solace are producing guidance for Local authorities, these will give more detailed guidance on what is required to be done by local authorities to comply with the Data Handling guidelines.

besafe.besure becrypt

NLAWARP PO Box 6733 Chingford, London E4 8UD Tel: 020 8524 2185
www.nlawarp.gov.uk Contact: mark.brett@socitm.gov.uk

BeCrypt Limited, Wyvols Court, Swallowfield, Berkshire, RG7 1WY
Tel: 0845 838 2050 email: info@becrypt.com www.becrypt.com

© 2008 Copyright of this document is owned jointly by Socitm and BeCrypt.

Non-Commercial and Public sector organisations may reproduce the contents of this document, so long as the source and copyright owners are acknowledged.

¹ Downloadable copies of the reports are available from www.becrypt.com