The Role of the Information Asset Owner: a Practical Guide
## CONTENTS

1. **Introduction** ................................................................................................................................. 4
   1.1 What is the purpose of this guidance? .......................................................................................... 4
   1.2 Who is this guidance for? ............................................................................................................... 5

2. **Just appointed?** .................................................................................................................................. 6
   2.1 First steps ........................................................................................................................................ 6
   2.2 Key principles ............................................................................................................................... 6
   2.3 What is an information asset and what assets are you responsible for? ...................................... 7

3. **Information risks to manage** ......................................................................................................... 8

4. **Your responsibilities** ...................................................................................................................... 9
   4.1 Lead and foster a culture that values, protects and uses information for the public good ............... 10
   4.2 Know what information the asset holds, and what information is transferred in or out of it........... 11
   4.3 Know who has access and why, and ensure their use of the asset is monitored ......................... 14
   4.4 Understand and address risks to the asset, and provide assurance to the SIRO ......................... 14
   4.5 Ensure the asset is fully used for the public good, including responding to access requests ................................................................. 17

5. **Scenario and case study** ............................................................................................................... 18

6. **Further reading** ............................................................................................................................ 19

Appendix A: Data Protection Principles ............................................................................................... 20

Appendix B: Principles on the transfer of information or responsibilities ........................................... 21
1. Introduction

The Information Asset Owner (IAO) is a mandated role, and the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

An Information Asset Owner is appointed by, and reports to, a Senior Information Risk Owner (SIRO), who in turn reports to the Accounting Officer or the Chief Executive. Information handling is reported on in your organisation’s statement of internal control, and the IAO is expected to provide information to go into that report.

The role was created following the Government’s Review of Data Handling in Government (DHR) in June 2008, which also established mandatory minimum measures for personal data handling in Government. You can find full details in HMG IA Standard No 6: Protecting Personal Data and Managing Information Risk. This incorporates the Data Handling Review and included and replaces the minimum mandatory measures.

Although it was created out of the DHR, which initially focused on personal data handling, the role is equally important for any sensitive information processed by your organisation, whether or not it includes personal information. The IAO also needs to manage information assets to comply with statutory obligations (such as Freedom of Information, the Public Records Act and the Data Protection Act).

Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information you hold, how important it is, how sensitive it is, how accurate it is, how reliant you are on it, and who’s responsible for it. It helps ensure that you can use the information you need to operate transparently and accountably, for example to meet open data standards, to unlock previously unavailable data and to improve public service.

1.1 What is the purpose of this guidance?

---

1 https://cesgiap.gsi.gov.uk/ia-policy-portfolio/docs/hmg-ia-standards/ias4-supplement6.pdf (Site requires registration)
3 Public Record Act 1958 nationalarchives.gov.uk/policy/act/
4 Data Protection Act www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
The three documents above give an overview of why the IAO role was created and what you are expected to achieve. But Information Asset Owners have asked for more information about what that might mean in practice. This document provides a good starting point for IAOs, giving practical guidance on:

- identifying information assets
- managing information risks
- your responsibilities
- how to achieve them
- who can help you
- how to know if you are doing your role well.

It fits into a wider package of support for your role, for example baseline training for IAOs, knowledge-sharing events, and continuing work to help define what we mean by an information asset.

1.2 Who is this guidance for?

This guidance is primarily aimed at Information Asset Owners. It may also be useful for Senior Information Risk Owners (SIROs) when appointing IAOs, and for information management (IM), information assurance (IA) and IT teams – for example Heads of Knowledge and Information Management, Departmental Record Owners, Heads of IT and IA – to help them to understand the support they may be called upon to provide.

It could also be useful for project managers when initiating projects, particularly those likely to be subject to Privacy Impact Assessments (PIAs), and to Departmental Security Officers (DSOs) who are responsible for all aspects of protective security.
2. Just appointed?

1.1 First steps

1. Have you done your baseline IAO training? This will give you an understanding of why your role is important, the risks you need to consider and who can help you. It’s an online package that will take just over an hour to complete. Baseline training is available from the Civil Service Learning website and may also be on your organisation’s website. As an IAO, you are required to successfully complete the Protecting Information Level 3 package, scoring at least 80% in the final assessment.

2. Have you attended any of the follow-up face-to-face training organised by The Cabinet Office?

3. Have you read Managing Information Risk? It gives a good overview of broader information risks, case studies, checklists and potential sources of assurance.

4. Have you contacted the other IAOs in your organisation to find out whether there is corporate information for IAOs on your intranet, or an IAO support network?

2.2 Key principles

Your role is about managing information not systems.

The initial driver for establishing the role of the IAO was to ensure that Personal Data (as defined in the Mandatory Minimum Measures, which have now been incorporated into HMG IIA Standard No 6) was identified and securely handled. However, you also need to ensure you are managing the handling of other categories of sensitive or important information that your organisation relies on too. This involves making sure that it can be used in the way that you need, for as long as you need.

You are responsible for ensuring that information is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards apply. But you are equally responsible for ensuring that its value to the organisation is fully realised, and that it is used appropriately, and within the law, for public good. You will also need to ensure that information is managed appropriately following change (see Appendix B).

---

5 Civil Service Learning
https://civilservicelearning.civilservice.gov.uk
Your role is about providing assurance and making sure that action is taken. But that doesn’t mean you have to do everything yourself – in fact, much of the role is about understanding and where necessary coordinating the activities of others in your organisation who have specialist areas of responsibility. Your IT, Security\(^7\) and IM functions are key contacts in supporting you in the role. However, if you delegate responsibility for ensuring actions are taken, you must make sure that this is properly co-ordinated and that there are clear reporting chains that everyone understands. You can delegate responsibility to particular areas that can support you in your role but you and your SIRO retain the accountability for proper information management and handling.

You may need to work with other IAOs in your organisation to ensure your information is properly protected and their value to the organisation fully realised.

### 2.3 What is an information asset and what assets are you responsible for?

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Your SIRO will decide what information assets you are responsible for. This should not just be a list of systems to manage, but should focus on the information that needs to be managed within those systems. This could cover both sensitive personal data and non-personal information that is critical to business. It could be held in paper as well as electronic formats.

When you are appointed you need to discuss and agree performance metrics. Some of these will be directly related to the need to demonstrate compliance with mandatory requirements to central government, but others may be specific to your organisation. Where practical, you should discuss with your SIRO what you will be expected to report back on.

---

\(^6\) See Managing Information Risk nationalarchives.gov.uk/documents/information-risk.pdf

\(^7\) Departmental Security Officers’ responsibilities are set out in HMG Security Policy Framework 1.0
3. Information risks to manage

As an Information Asset Owner you will need to assure against:

- inappropriate access to, or disclosure of, protectively marked or personal data by staff, contractors and outsiders, whether accidental or deliberate
- internal threat – staff acting in error or deliberately, or external parties getting your information illegally and exposing it/acting maliciously to defraud you or your customers
- information loss – particularly during transfer or movement of information, or as a result of business change
- loss of ready access to information
- loss of digital continuity – i.e. losing the ability to use your information in the way required when required. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information – and how long you need to use and keep it – is often different to the lifecycle of the IT system that we have to access and use it
- poor quality of information and poor quality assurance, for example, of datasets
- poor change management – business needs change, systems change, your information risk appetite may change, so you need to keep your policies and processes in step accordingly
- not maximising the public benefit from information (leading to a waste of public money and poor service delivery).
4. Your responsibilities

Your role is to ensure that the information in your charge is properly protected and its value to the organisation fully realised. This section of the guidance looks at what you are required to do to achieve these responsibilities, and how that might look in practice. Some of your responsibilities require you to take action, others simply to assure that action is being taken by others (such as your IT, IM and IA teams).

You have five responsibilities:

1. **Lead and foster a culture that values, protects and uses information for public good.**
2. **Know what information the asset holds, and what information is transferred in or out of it.**
3. **Know who has access and why, and ensure that their use of the asset is monitored.**
4. **Understand and address risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are appropriately managed.**
5. **Ensure the asset is fully used for the public good, including responding to access requests.**

You need to be able to answer the following questions:

- Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented and shared with your SIRO and others who need that information?
- Have I assessed and logged information risks to those assets?
- Do I have a plan for managing risks, and maximising opportunities for using my information assets for the public good?
- Do my team(s) and third parties understand their roles and responsibilities in managing those risks and opportunities?

Your IM, IT, IA and security teams are a great resource and can support you to provide much of that assurance. You need to tell them your business requirements so that they can include them into their operational IT, protective security and information management.
4.1 Lead and foster a culture that values, protects and uses information for the public good

<table>
<thead>
<tr>
<th>What you need to do</th>
<th>How you might do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Attend (and pass) training – when you’re appointed and annually (at a minimum)</td>
<td>• Sign up to the Cabinet Office mailing list (<a href="mailto:isa@cabinet-office.x.gsi.gov.uk">isa@cabinet-office.x.gsi.gov.uk</a>) to receive updates on training and knowledge sharing events</td>
</tr>
<tr>
<td>• Actively contribute to your department’s plans to achieve and monitor the right information handling culture</td>
<td>• Meet with other IAOs in your organisation to share ideas and talk to your Knowledge and Information Management team</td>
</tr>
<tr>
<td>• Ensure the handling of your information assets complies with the Data Protection Act and your department’s compliance mechanisms and policies</td>
<td>• Join the Information Assurance community on Civil Pages (<a href="http://www.civilpages.gsi.gov.uk">www.civilpages.gsi.gov.uk</a>)</td>
</tr>
<tr>
<td>• Understand and document the business value of the information assets you are responsible for</td>
<td>• Make sure that people who use your information assets understand the rules and are aware of the consequences of non compliance. Explore using line management responsibilities – appraisals and objectives setting – to monitor this</td>
</tr>
<tr>
<td></td>
<td>• Talk to your SIRO about what you can do to contribute to departmental plans for culture change</td>
</tr>
<tr>
<td></td>
<td>• Set up a ‘lessons learned’ log, so if things go wrong you can learn from them and ensure that policies and practices are changed</td>
</tr>
<tr>
<td></td>
<td>• Talk to your Departmental Security Officer (DSO) to ensure appropriate physical, procedural and personnel security</td>
</tr>
</tbody>
</table>

Get assurance from others:

You can talk to your Data Protection teams and FOI teams to assure that how you’re managing your information assets meets requirements.

You can also contact relevant teams to get the assurance that the way you need to use your information assets is reflected in IM, IA, IT and protective security policies and practices.
### 4.2 Know what information the asset holds, and what information is transferred in or out of it

<table>
<thead>
<tr>
<th>What you need to do</th>
<th>How you might do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Understand and address risks to your information assets, and provide assurance to your SIRO</td>
<td>• Document your understanding of your information assets (in a simple spreadsheet, or using existing spreadsheets such as an Information Asset Register(^8)). Work with your IT and IM teams to document:</td>
</tr>
<tr>
<td>• Know who has access to your information assets and why, and monitor use</td>
<td>o what the assets are – what they cover, their content, what’s sensitive and/or protectively marked and what personal data you’re responsible for</td>
</tr>
<tr>
<td>• Understand whether a delivery partner or supplier has a dependency on your information to deliver a service</td>
<td>o the value of your information assets to the business – now and in the future. How important are they, and why? What would be the impact of losing or mishandling them? As part of this process you should consider the benefits of increasing access, or of information re-use</td>
</tr>
<tr>
<td>• Approve and minimise transfers</td>
<td>o your usability requirements for those assets – who needs to be able to find them, how do you need to work with them, to maintain the understanding and trust of that information? What retention and disposal schedules do you need?</td>
</tr>
<tr>
<td>• Monitor the allocation of users’ rights to transfer personal information to removable media</td>
<td>• Make sure your information assets are fully used for the public good, including responding to access requests. This includes actively considering whether public protection or public services could be enhanced through greater access to the information assets that you’re responsible for.</td>
</tr>
<tr>
<td>• Approve arrangements so that information put onto removable media is minimised and protected</td>
<td>• Keep a record of all staff and contractors with access to records containing personal data – or who handle records containing personal data. Ensure a process is in place to remove that access as soon as it is no longer required</td>
</tr>
<tr>
<td>• Make sure your information assets are fully used for the public good, including responding to access requests. This includes actively considering whether public protection or public services could be enhanced through greater access to the information assets that you’re responsible for.</td>
<td>(^8) See Identifying Information Assets and Business Requirements <a href="http://nationalarchives.gov.uk/documents/identify-information-assets.pdf">nationalarchives.gov.uk/documents/identify-information-assets.pdf</a></td>
</tr>
</tbody>
</table>
• Manage agreements on the sharing of personal information between organisations
• Keep written records of the decisions you agree with your IM, IT, IA and security teams
• Talk to your DSO about information security

Get assurance from others:
Get assurance from your IT and IM teams that they are managing digital continuity – the ability to use your information assets in the way that you need, for as long as you need. The National Archives has produced guidance that will help them to do this, available at nationalarchives.gov.uk/digitalcontinuity.

Get assurance from your Departmental Security Officer (DSO) that personal and protectively marked information (digital and paper) is appropriately protected.

This should cover:
• the unavoidable use of removable media
• mandatory risk mitigation measures if use of removable media is unavoidable
• alternatives to removable media for information transfer or storage
• suitable security configurations on remote systems with approved access to the information assets you are responsible for
• the secure disposal of personal data and protectively marked information
• exemptions from the requirement to encrypt material stored on removable media, together with approval of compensating risk management measures.
## Helpful hints: fields you could use in your Information Asset Register

| Description | Brief description of what the asset is  
More detail on what the components of the asset are |
|-------------|--------------------------------------------------|
| Users       | Who created the asset, or where does the asset come from?  
Who is the Information Asset Owner?  
Which department holds responsibility for the asset?  
Who are the stakeholders? |
| Date        | Creation date  
Date closed (for closed assets)  
Last date asset register was reviewed/updated |
| Asset Status| Is this asset being actively updated?  
Has the asset been closed? |
| Purpose     | What part of the business does this asset support?  
Business risks from or to the asset |
| Value       | What is the value to the business?  
What would be the cost of replacing the information? |
| Retention schedule | How long should it be kept in immediate access?  
What should happen to it when it no longer needs immediate access?  
What are the disposal requirements? |
| How do you need to use your asset | How will you find the information?  
Who can access the information and how?  
What do you need to be able to do with the information?  
What do you need to be able to understand about your information?  
To what extent do you need to prove your information is what it claims to be? |
| Risk        | What are the risks to the asset?  
What are the risks to the business from the asset (for example from its loss, corruption or inappropriate access)? |
4.3 Know who has access and why, and ensure their use of the asset is monitored

<table>
<thead>
<tr>
<th>What you need to do</th>
<th>How you might do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Agree in writing that relevant access control regimes allow business to be transacted with an acceptable level of risk – or require that an acceptable alternative approach be adopted. You need to agree who has access to your information assets</td>
<td></td>
</tr>
<tr>
<td>• Ensure that you keep a record of individuals with access to, or who handle, records containing personal data</td>
<td></td>
</tr>
<tr>
<td>• Keep a log of access requests</td>
<td></td>
</tr>
<tr>
<td>• Make sure you understand your organisation’s policy on the use of the information assets you are responsible for</td>
<td></td>
</tr>
<tr>
<td>• Put in writing to your SIRO that access provided is the minimum necessary for business purposes – or request an alternative</td>
<td></td>
</tr>
<tr>
<td>• Talk to your DSO to ensure appropriate policies to protect physical, personnel and information security are in place</td>
<td></td>
</tr>
</tbody>
</table>

Get assurance from others:
You don’t have to monitor access directly but you do need assurance that it is being done. Agree how to monitor usage with your managers and then ask them for records of usage checks and summary reports on what’s been done, and the results.

Get assurance from your IT team that access rights to IT systems are limited to the appropriate people.

4.4 Understand and address risks to the asset, and provide assurance to the SIRO

<table>
<thead>
<tr>
<th>What you need to do</th>
<th>How you might do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure that significant correspondence about information risk handling are placed on the corporate record</td>
<td></td>
</tr>
<tr>
<td>• Contribute to the department’s risk assessment. To do this, the IAOs</td>
<td></td>
</tr>
<tr>
<td>• Make sure you are aware of the full range of risks – see section 3 above</td>
<td></td>
</tr>
<tr>
<td>• You defined your usability requirements in section 4.2 above. Use this information to assess risks and opportunities:</td>
<td></td>
</tr>
</tbody>
</table>
should identify and, where appropriate, formally accept significant risks introduced when personal information is moved from one organisational unit, system element, medium or location to another.

- Make the case where necessary for new investment to protect the asset.
- Ensure all risk decisions taken are demonstrably in accordance with departmental risk management policies established by the SIRO.
- Make risk decisions where users believe it is not possible to comply with policies or controls, consulting others as necessary, and ensuring the decision and the reasons behind it, are placed on the corporate record.

<table>
<thead>
<tr>
<th>should identify and, where appropriate, formally accept significant risks introduced when personal information is moved from one organisational unit, system element, medium or location to another</th>
<th>understand how to maintain your digital continuity – identifying the management processes and technologies you need to satisfy your usability requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make the case where necessary for new investment to protect the asset</td>
<td>identify the technology that your information is dependent on to remain usable. Where are the assets held, and which search tools enable their discovery?</td>
</tr>
<tr>
<td>Ensure all risk decisions taken are demonstrably in accordance with departmental risk management policies established by the SIRO</td>
<td>identify the risks to the information asset that could arise from changes, for example technology change (changing suppliers, systems and so on) and organisational change (e.g. sharing agreements, who has access to the information)</td>
</tr>
<tr>
<td>Make risk decisions where users believe it is not possible to comply with policies or controls, consulting others as necessary, and ensuring the decision and the reasons behind it, are placed on the corporate record</td>
<td>read your organisation's Information Risk Policy – a mandatory document for all government departments and agencies. This should indicate where losses of confidentiality, integrity and availability are likely to have the most critical impacts on your business, and where the greatest proportion of your mitigation should be focused</td>
</tr>
<tr>
<td></td>
<td>talk to your SIRO about how the risk policy applies to the information assets you are responsible for</td>
</tr>
</tbody>
</table>
Get assurance from others:
Ensure your IM and IT teams carry out regular digital continuity risk assessments and work with you to ensure your continuity requirements are well defined – this will provide you with the assurance that your information assets can be used in the way that you need, for as long as you need. Your IM and IT teams may also be able to give you some audit data on how your information assets are being used and protected.

Helpful hints: look at the systems that your information assets are contained in. Here are some risk areas:

**Databases:** is it easy to know who has access, or to identify what is personal data? Is the management of databases consistent? If your protocols for protecting personal data differ across databases, why is this?

**Inappropriate access to shared drives:** who has access to information assets on shared drives and why? Do you know what sensitive personal data is held there? Do you have arrangements for protecting it?

**EDRMS:** are access controls being applied properly and consistently to information assets in your EDRMS?

**Search capability:** can you find the right information easily in the systems that hold it?

**Email:** is your email protectively marked? Where are emails stored and how are they protected?
4.5 Ensure the asset is fully used for the public good, including responding to access requests

<table>
<thead>
<tr>
<th>What you need to do</th>
<th>How you might do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure you are able to use your information assets as appropriate to comply with Public Data and transparency requirements⁹</td>
<td>• Identify which of the datasets you’re responsible for are Public Data (see <a href="http://data.gov.uk">http://data.gov.uk</a>). Public Data is the objective, factual, non-personal data on which public services run and are assessed, and on which policy decisions are based, or which is collected or generated in the course of public service delivery.</td>
</tr>
<tr>
<td>• Regularly review whether you could make better use of the information assets you are responsible for</td>
<td>• Submit potential Public Data to your Department’s Transparency Practitioner (a list is available on the Making Public Data Public community on Civil Pages).¹⁰</td>
</tr>
<tr>
<td>• Manage and approve agreements on sharing personal information between organisations and ensure access decisions are taken accordingly</td>
<td></td>
</tr>
<tr>
<td>• Log access requests from others</td>
<td></td>
</tr>
</tbody>
</table>

Get assurance from others:

You should get assurance from your Freedom of Information Management teams and transparency managers that they are managing the digital continuity of the information assets you manage – so that you are assured that your information assets can be used in the way that you need for as long as you need. You should also receive and log access requests from others. To do this, you must ensure that a log of access requests is maintained.

You should ensure that when public access to information is in the public interest, this is reflected in your Departmental Freedom of Information Publication Scheme.

---

⁹ See the government’s Coalition programme, *The Coalition: our programme for government*, p 21 [www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf](http://www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf)

¹⁰ Making Public Data Public, Civil Pages [www.civilpages.gsi.gov.uk/display/makingpublicdata/Home](http://www.civilpages.gsi.gov.uk/display/makingpublicdata/Home)
5. Scenario and case study

The following provide examples of what needs to be done in relation to understanding and addressing any risks to your information assets (see section 4.4).

**Scenario:** you are responsible for information previously used in response to a Parliamentary Question (PQ). This information is unlikely to be sensitive as it is now in the public domain. But if you can’t get reliable access to previous answers to PQs when you really need it — and to tight PQ deadlines — you are at risk of publishing something that’s inconsistent with your previous stated position. Your risk mitigation therefore needs to focus more on the integrity and availability of your information asset, and less on its confidentiality.

**Case study:** CESG, the National Technical Authority for Information Assurance needed to give access to technical policy, guidance and implementation documents to private-sector licensed information assurance practitioners. Some documents carried protective marking so could not be made available over the internet, and there were no approved encryption products available. The IAO needed to decide how to handle these assets, balancing the need for access with the need for protection.

They started by assessing the value of that information. Without access to the entire portfolio, practitioners could not do their job properly, which could lead to poor system security in parts of government. As no technology solutions were available, the IAO looked at procedural measures to mitigate the risk.

Consultants operated across the county so requiring them to personally pick up a CD was not a cost effective option. The IAO consulted local security experts to understand the basic handling requirements in the Security Policy Framework and agreed that CDs could be sent out using approved courier channels, with positive confirmation of receipt. As an additional check, practitioners were notified in advance that a CD would be sent, and were asked to indicate whether they would be available to take delivery of it. Those who could not guarantee being able to receive it were sent a copy later, when receipt could be immediately assured.
6. Further reading

For more information about how you can assure against the risk of losing the use of your information assets over time and during periods of change, visit nationalarchives.gov.uk/digitalcontinuity.

For more on why it matters, read What Does Digital Continuity Mean for You? An Overview of the Benefits


Managing Information Risk gives a good overview of broader information risks, case studies, checklists and potential sources of assurance

nationalarchives.gov.uk/documents/information-management/information-risk.pdf
Appendix A: Data Protection Principles

Guidance on the Data Protection Act should be obtained from the Information Commissioner’s Office (www.ico.gov.uk) and from departmental data controller staff. The eight principles identified in the Data Protection Act 1998 are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   a. At least one of the conditions in Schedule 2 is met; and
   b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. 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.

8. Personal data shall not be transferred to a country of territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Appendix B: Principles on the transfer of information or responsibilities

Making arrangements for the transfer of information, records and knowledge is a key part of any machinery of government change. However, all too often this aspect is not properly planned for, inadequately resourced and left until it is too late to do everything that needs to be done. Listed below are the eight basic principles that should be followed for a successful transfer.

Further detail on all these areas can be found in The National Archives' Machinery of Government Changes: Guidance on the Transfer of Records, Information and Knowledge. nationalarchives.gov.uk/documents/information-management/machinery_of_government.pdf

Reinforce Senior Management support

Ensure that senior management understand what needs to be done (including setting an appropriate budget) and the risks to the business if the transfer is not carried out successfully. Failure to transfer information and knowledge effectively between departments can make it impossible to maintain business continuity and can result in the loss of vital information, loss of functionality of digital information, inability to be transparent and accountable and meet legal obligations, inefficiency and substantial additional costs.

Plan in advance

Start planning for the transfer of information as soon as notification that the organisation/function is to be abolished or transferred has been received. Identify desired outcomes – especially the usability of information (or digital continuity requirements after transfer) and test progress against these.

Clarify who is responsible

Establish as early as possible who is going to do the work and form a joint Information Transition Team. Ensure that transferring and receiving bodies and any contractors employed in information related activities (for example, an IT service partner) have a clear understanding of their separate and joint roles and responsibilities.
Decide what to transfer

Decide what information needs to be transferred and to where, for example, information of continuing business or legal value will need to be identified and transferred to the department that is inheriting responsibility for the function/s. Information of archival value may be transferred to The National Archives. Consider information/records in all forms, for example, paper files, information within an electronic records management or email system, websites, intranets, shared drives, databases AND accompanying information such as finding aids, Information Asset Registers or retention/disposal information.

Make provision for the continuity of digital information

Define the usability requirements for information to be transferred, and test against them throughout the transfer process. The receiving organisation needs to ensure the information can be found, opened, used, understood and trusted as required and will need to ensure it receives both files and necessary contextual metadata and has the technology to enable the usability requirements to be met.

Ensure continued compliance with legislation and information security

Clarify responsibilities for Freedom of Information and Environmental Information requests and related complaints and appeals and ensure that handover or guidance notes are prepared. Comply with rules on information security when transferring information and records and conform to the Security Policy Framework for protectively marked material.

Capture knowledge and communicate to staff and stakeholders

Capture the knowledge of staff from the transferring organisation, particularly if they are not transferring with the function and make as much information as possible about the changes available to staff in both organisations. Plan communication with customers and end-users.

Take advantage of opportunities for savings and increased efficiency

Capitalise on opportunities to increase efficiency and make savings, for example, shared service options could be considered for storage/electronic systems, information that is not required could be deleted rather than transferred.