IT asset disposal for organisations

Data Protection Act

Contents

Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers fully understand their obligations and promote good practice.

This guidance explains to data controllers what they need to consider when disposing of electronic equipment that may contain personal data.

Overview

You should:

- ensure that the responsibility of asset disposal is assigned to a member of your staff with a suitable level of authority;
- complete a full inventory of all equipment that you have marked for disposal;
- be clear about what will happen with devices when you no longer need them;
- consider the security vulnerabilities associated with each method of disposal;
- ensure you delete personal data before recycling devices, so that data is not accessible to others after the device has left your ownership;
- be aware that any specialist service provider you use will be considered to be a 'data processor' under the DPA; and
- have a written contract in place between you and the data processor, ensuring that there is an appropriate level of security in place.

What the DPA says

> The seventh principle says: appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data.

It means you must have appropriate security in place to prevent the personal data you hold from being accidently or deliberately compromised. This is relevant in the IT asset destruction and recycling processes.

More information can be found in the seventh principle section of our Guide to Data Protection.

In general, this means you should:

- design and organise your security to fit the nature of the personal data your organisation holds and the harm that may result from a security breach;
- be clear about which member of its staff in your organisation is responsible for ensuring information security;
- make sure you have the right physical and technical security measures in place, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

If personal data is compromised during the asset disposal process, even after it has left your organisation, you may still be responsible for breaching the DPA so it is important to manage the process correctly.

Create an asset disposal strategy

Add a section to your security policy that addresses the process of IT asset disposal and personal data deletion. Consider the following points when creating your strategy:

How will devices be disposed of when no longer needed?

Be clear about what will happen with devices that are no longer needed. Will they be made available for reuse or will they be

recycled, or destroyed? Consider how IT assets will be removed from your organisation and who will be involved in this process.

Conduct a risk assessment of the disposal process

Whether you decide to use a specialist asset disposal service provider or delete personal data yourself before recycling, it is important to consider the security vulnerabilities associated with each method of disposal.

You may recycle usable equipment, donate it to another user or return leased equipment to the owner. You may decide that you can delete personal data within your organisation before recycling equipment and devices but using a specialist service provider is also an option. In all circumstances, it is important to consider what personal data may be leaving your organisation along with the device it is stored on. Your risk assessment should consider the process of handing your equipment to a third party and you should always be aware, and make a written record, of who you are handing the devices to.

More details can be found in the Selecting an IT asset disposal company section below.

Identify the devices containing personal data

Much of your data may be stored on PCs and laptops but think about other devices that store electronic data such as printers, faxes, servers, smartphones, tablets and USB or backup storage. If you are not using a specialist service provider to recycle your IT assets, make sure you wipe personal data before recycling, so that it is not accessible after it has left your organisation. Some of the techniques in our Deleting personal data guidance may suit your organisation's requirements.

Update your security policy as your organisation begins to use new devices that are capable of storing personal data so that you can dispose of these securely, when needed.

Categorise the personal data

The DPA says that you should have a level of security in place that is appropriate to the nature of the information you hold and the harm that might result from its improper use or accidental loss or destruction.

Consider using a third party service provider

If you choose to use a specialist service provider to remove your IT assets, make sure you include clear details in your security policy about how the chain of custody is to be managed. Devices should not leave your organisation before you have established who is responsible for deleting the personal data contained on them, whether that is someone within your organisation or the specialist third party provider as part of its service.

Selecting an IT asset disposal company

If you use a specialist asset disposal company to recycle your old electronic equipment it will be defined as a 'data processor' under the DPA. As the asset disposal company will be acting on your behalf, you will be responsible under the DPA for what the provider does with any personal data contained on the devices that it is recycling. If the provider does not successfully delete personal data that is subsequently compromised you may be responsible for the breach. Read further guidance on the relationship between a data controller and a data processor in Identifying data controllers and data processors.

Choose an IT asset disposal company that provides sufficient guarantees about its security measures. You should be satisfied that your service provider will treat the personal data with the same level of protection, or better, as you.

Look for independent approval of products used in the deletion process such as CESG, the UK government's national technical authority for information assurance.

If possible, conduct a client site assessment and audit of your chosen disposal company. Continue to audit the data processor for compliance throughout the business relationship.

Draw up a contract with the data processor

The DPA sets out that a written contract must be in place between your organisation and the data processor, so that both parties are aware of their obligations. Ensure that your contract includes:

- explicit direction on the services to be undertaken and that it may only act in accordance with your instructions;
- an approved specification for IT asset disposal which is aligned to your disposal/security policy; and

- full details of all downstream partners involved in the service. Any downstream partner contracts should include the same data controller specification for IT asset disposal as the minimum service level to be met.

Manage the asset disposal process and data processors

Complete a full inventory of all equipment that is marked for disposal. As noted above, you should maintain a written record of all equipment transferred to your service provider if you are using one.

Monitor and audit your service provider regularly to ensure that it is complying with your instructions, putting its security measures into practice and maintaining the expected service quality by establishing an on-going audit process.

If you lease equipment such as printers, check what the leasing company will do with the equipment when it is returned. In particular, check to see if it wipes personal data from devices before these are resold or recycled. You may need to delete information contained on the hard drives of items such as printers before they are returned to the leasing company and recycled.

Assign an asset disposal champion

Ensure that the responsibility of asset disposal is assigned to a member of your organisation with a suitable level of authority, as security measures can become flawed and out of date very quickly, particularly if there is no accountability within an organisation.

Your IT security manager might be suitable but, if you do not have one, make sure that someone is aware of which devices are leaving the organisation, what personal data is stored on them and who has responsibility for erasing the personal data.

Other considerations

Other relevant ICO guidance includes:

⇒ Deleting personal data

More information

This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please contact us: see our website www.ico.org.uk.