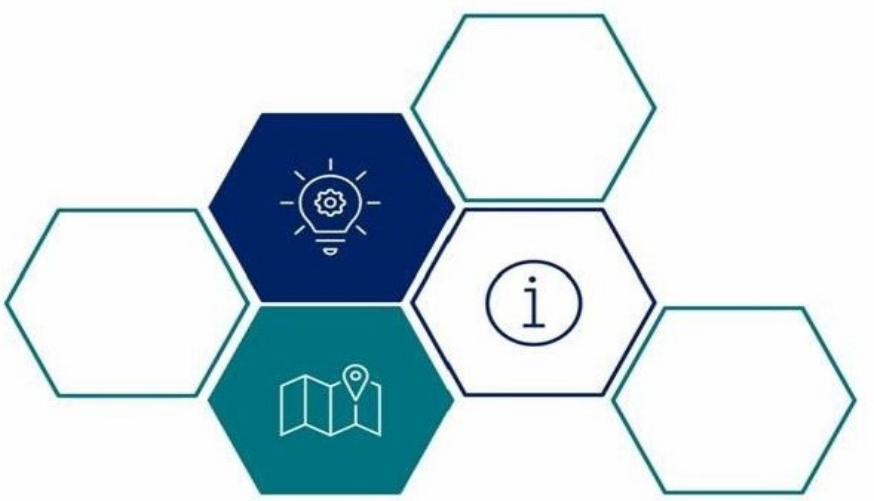
Data Protection and PECR Training
Supporting notes and further reading
Module 1: Data protection definitions



Introduction

These notes are designed to set out the key points covered during module one of our DP and PECR online training programme. This module, alongside modules two and three, will also prepare you for workshop on one personal information and the lawful bases. These notes aren't designed to replace the online module but are intended to be a point of reference for your follow-up study. You may find it helpful to have these notes open whilst watching the online module.

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA)

Remember: The Data (Use and Access) Act (DUAA) made some amendments to these laws but does not replace the information protection legislation.

This document contains:

- Supporting notes
- Optional further reading

Supporting notes

Module one covers key information protection definitions found in article 4 of the UK GDPR and part 1 of the DPA. These are:

- Personal information
- Pseudonymisation and anonymisation
- Information which falls under the legislation
- Processing
- Personal information breach
- Health and social work professional, recipient, accuracy
- Controllers and information processors
- Joint controllers

Personal data

Personal data is any information relating to an identified or identifiable living person, also known as a data subject.

A deceased person isn't a data subject and information relating to them doesn't fall under the information protection legislation.

We usually refer to 'personal information' and 'person' or 'people' for simplicity.

In many cases it is clear – there is no doubt that information such as your name, qualifications, salary, address and hobbies is about, and related to, you.

The key questions are:

- Can a person be identified from the information?
- Does the information relate to an identifiable person?

In most cases the information will obviously be about a person who can be identified from it.

For example, the ICO holds my personal information in a record which includes my name, job title and salary.

If you can distinguish a person from other people, then that person is 'identified' or is 'identifiable'.

Other examples include:

- my council tax bill with my name and address, as my name together with this information will be sufficient to identify me;

- my manager's opinion of me in a performance review;
- my social media username or 'handle' as this is 'a common identifier' named in the UK GDPR; and
- a complaint about my work. Note this will be my personal information because it relates to me, but it will also be the personal information of the complainant.

This means that whether information is personal information depends on the context.

In some circumstances, information may not be personal information – like a job advert with a starting salary which doesn't relate to anyone.

But in other circumstances, if the same salary details are linked to a name (for example, when the vacancy has been filled and there is a single named person in post), the salary information about the job is personal information 'relating to' that employee.

It's not always obvious when information is personal information but there are key points you should consider:

- the context in which the information is held;
- whether the person is really the focus of the information;
- what the information actually tells you about the person;
- whether the information is being used in a way that might have an impact upon the person; and also
- whether the information is that of a sole trader or a limited company.

Finally, information about a sole trader is personal information but information concerning a limited company isn't.

Example - personal information in a hospital complaints file detailing an investigation into a complaint about standards of care

This comes up a lot – we often get complaints about requests for personal information held in complaints files.

- Imagine a person makes a complaint to a hospital about the standards of care in a ward and about a particular nurse.
- The hospital creates a complaint file and conducts an investigation.
- The person who made the complaint then requests a copy of the file because they want to know what has happened.

- However, just because someone makes a complaint, this doesn't mean that the whole complaint file will be their personal information.
- The details of the complaint itself will be the complainant's personal information.
- Any disciplinary steps taken against the nurse as a result of the complaint would not be the personal information of the complainant.
- A note on the file explaining that the complainant was removed from the premises because of threatening behaviour is that person's personal information because it relates to them.
- If some of the information in the file is about general standards of care on the ward then it won't relate to any one person and so won't be personal information at all.
- So in this situation, the organisation must identify the personal information and decide who the information subject is for each piece of information.

Example - personal information in a meeting note held by a business, recording an employee's attendance and contributions in a work meeting

- Hopefully it's clear that the list of attendees at the meeting is the personal information of identifiable people.
- However, an employee's contribution to a meeting is more debatable.
- If the people in the meeting discuss and record details about the employee's poor performance, then this is that person's personal information.
- The employee's opinion about a new project is their personal information.
- If the meeting note records that the employee in the meeting merely explained the company's policies, their contribution doesn't relate to them and so isn't their personal information.

There is a more in-depth discussion of the issues surrounding patient confidentiality and authority to act on behalf of someone else (for example if the complaint is about the treatment of a relative) in our guidance.

For example, if the information subject is deceased then the Access to Health Records legislation applies rather than information protection legislation.

Controllers and data processors

A controller is a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information.

For the purposes of this training, we use the term 'organisation' as a plain-language alternative to 'controller.' While 'controller' is the correct legal term, we use 'organisation' throughout this training for simplicity.

A data processor is a person, public authority, agency or other body which processes personal information on behalf of the controller.

For example, the ICO is a controller and processes our personal information. It may send out our payroll details to be processed by another company and that other company is a data processor who handles the information on behalf of the ICO. But it's the ICO as the controller who determines the purpose and means of the processing.

Processor obligations are set out in the guidance and in article 28, including the requirement for a contract.

Example - controller and data processor

A local council wants to promote recycling in its area and contracts a private company to send out mailings to local residents to encourage them to support the initiative.

- The council gives the company a copy of its database of names and addresses. The company then uses this information to send the mailing out and record any responses.
- In these circumstances, the council is a controller because it's determining the purpose for which the information is being processed and the means of the processing.
- The private company is a data processor because it's processing the information on behalf of the council (and following the council's clear instructions). It isn't a controller because it has no say in either the purpose for the processing or the means of processing.
- The controller must have a contract in place with the processor.
- If the company starts to process the information for its own purposes, it will become a controller.

Joint controllers

In other circumstances, two or more controllers might act together to decide the means and purpose of the processing and in this case, they would be joint controllers.

The obligations of joint controllers are set out in article 26.

Example - joint controllers

Two shops might decide to work together on a sales promotion.

- They amalgamate their customer databases and send out a joint promotion to both sets of customers.
- They are joint controllers because they are acting together to decide the purpose and means of the processing.

Two organisations who share personal information might remain as separate controllers if they process the information for different purposes.

Processing

Processing is any operation or set of operations which is performed on personal information or sets of personal information, whether or not by automated means.

These operations include the collection, organisation, storage, retrieval or use of data.

Remember, for simplicity, we usually say 'using' or 'handling' 'personal information'.

A personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

So, it's a security incident that affects the confidentiality, integrity, or availability of personal information. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about the disclosure or loss of personal information.

A breach of other parts of data protection law isn't a personal data breach.

Examples of personal data breaches

- a politician leaving a file on a train;
- a teacher leaving a confidential file on a photocopier;

- a social worker sending a child's sensitive personal information to the wrong person;
- a medical employee accessing a patient's file without permission;
- a bank losing a CD containing customer bank details; and
- an ICO caseworker sending details of a complaint to the wrong organisation.

In all these circumstances, we would expect the organisation to consider whether the breach should be reported to us. For example, we have internal procedures in place for circumstances where a caseworker sends information to the wrong organisation.

The organisation should notify the ICO of any personal information breach unless it's unlikely to result in a risk to the rights and freedoms of people.

Data processors must also inform organisations of any breach.

Pseudonymisation and anonymisation

Pseudonymisation is a key measure in the UK GDPR which can be used to ensure security of processing.

It's a technique organisations can apply to personal information, so it doesn't identify a specific person without using additional information. The additional information – or key - is usually held separately within the organisation. Pseudonymised information remains personal information and is still subject to the UK GDPR.

This contrasts with anonymisation which is where the means of identity are removed altogether.

For example, I may be referred to as 'patient 51' in a hospital document, but the hospital is able to look up patient 51 and identify that it is me. For the purposes of that document, I have been pseudonymised. But if the hospital has no way of telling who patient 51 is, then the information has been anonymised.

Information that's been truly anonymised isn't personal information and the UK GDPR doesn't apply.

Information which falls under DP legislation

The legislation applies to the processing of all personal information held on a computer in electronic format.

It also applies to manual information when held in a structured filing system. Manual information is paper-based information.

A filing system is any structured set of personal information which is accessible according to specific criteria. A filing cabinet containing files ordered alphabetically or in chronological order is a structured filing system and falls under the legislation.

It also applies to information intended to form part of a filing system. This means that information protection applies to a list of names in a set of notes which is about to be filed or input onto a computer.

If the organisation holds what we call manual unstructured information – let's say piles of paper it has never filed and has no intention of filing – then the UK GDPR and the DPA do not apply to this information - unless the organisation is a public authority (PA).

If manual information isn't structured and it's held by a PA, different conditions apply because a public authority is subject to the Freedom of Information Act (FOIA).

If you need to find out more about this, please refer to the data protection guidance for more information.

Back to top

Optional further reading

Our website

Go to the homepage of the ICO website and click on 'For organisations'.

A link to UK GDPR Guidance and resources is found on this page. Note, there are also links to guidance for the other legislation we regulate.

From here, have a look at the following pages:

- 'Personal information -what is it?'
- 'Controllers and processors'
- 'Security, including cyber security'

Back to top

KNOWLEDGE SERVICES

UPDATED: 4 February 2026