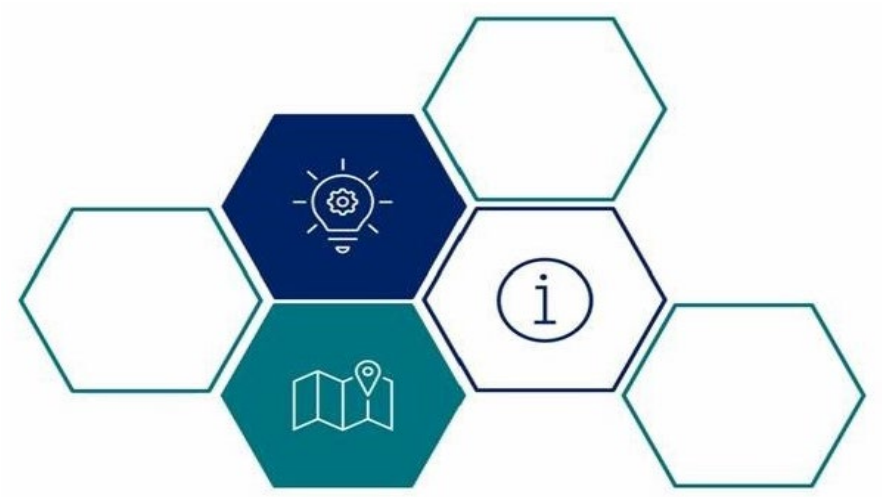
Data Protection and PECR Training

Supporting notes and further reading

Module 7 : Principles part 3 - security, accountability, and governance



Introduction

These notes are designed to set out the key points covered during module seven of our DP and PECR online training programme. This module, alongside module six, will also prepare you for workshop three on the data protection principles part two. 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 2025 (DUAA) made some amendments to these laws but doesn't replace the data protection legislation.

This document contains:

- Supporting notes
- Optional further reading

Supporting notes

Module seven looks at principle (f) (integrity and confidentiality) and an organisation's accountability and governance obligations. It covers:

- Principle (f) – integrity and confidentiality
    - Risk assessments, security policies and measures
- Accountability
- The accountability and governance provisions
    - Data protection by design and default
    - The Data Protection Impact Assessment (DPIA)
    - Recording personal data breaches (PDBs)
    - Documentation
    - The Data Protection Officer (DPO)
    - Codes of conduct
    - Certification
- The security and accountability obligations of the data processor

Principle (f) – integrity and confidentiality

A key principle of the UK GDPR is integrity and confidentiality, also known as the security principle. This principle is concerned with the broad concept of information security, including cybersecurity and organisational security.

Whilst article 32 of the UK GDPR provides specifics about the security of processing – eg, pseudonymisation. This article says that the level of security should be appropriate to the risk and include:

- pseudonymisation and encryption of personal data;
- the ability to ensure ongoing integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, and for keeping appropriate documentation to evidence this.

This allows the organisation to meet its key principle (f) obligations to protect the integrity and confidentiality of its personal data.

It also ensures the availability and resilience of its processing systems which might involve measures such as disaster recovery plans.

Organisations must put 'technical and organisational measures' in place to ensure an appropriate level of security to the risk posed by their use of information.

Organisations should also pay particular attention to the risk of unauthorised or unlawful processing and against accidental loss, destruction or damage of personal information.

Finally, where appropriate, organisations should use security measures such as pseudonymisation and encryption.

Risk assessments, security policies and measures

Organisations must consider the risk presented by their use of information and use this to assess the level of security it needs to put in place.

Organisations to think about the nature of the information and the consequences of losing it or of it being disclosed to the wrong people.

Recital 75 lists the types of personal information which are considered to be high risk. It includes special category data and criminal offence data.

This information risk assessment is key to the organisation's security considerations.

When deciding what measures to implement, the organisation may take into account practical issues such as available technology and the costs of implementation.

The kinds of policies an organisation should have in place and the measures it should implement are discussed in detail in our guidance. These include:

- having a risk register which identifies the processing risks and outlines how the organisation will mitigate against those risks;
- having a formal information security policy outlining responsible members of staff, rules for information handling and staff training;
- putting in place a business continuity policy which outlines how data will be protected and recovered;
- conducting internal audits of processing activities and their security; and

- reviewing access to premises or equipment.

Basic organisational measures such as regular staff training and clear policies on information handling are key to preventing data breaches.

Organisations should think about factors like:

- the quality of doors and locks, and the protection of their premises through the use of alarms, security lighting or CCTV; and
- how they keep their IT equipment, particularly mobile devices, secure.

Technical measures cover areas such as:

- physical security, for example, alarms, locks, and the disposal of data;
- computer security such as encryption, firewalls, and passwords;
- having anti-virus software; and
- having system backups in place.

Accountability

Accountability is the final data protection principle – it makes organisations responsible for complying with the UK GDPR and says they must be able to demonstrate their compliance.

So, organisations must put in place appropriate technical and organisational measures to meet the requirements of accountability.

And organisations must also review and, where necessary, update the measures they put in place.

Accountability and governance provisions

These provisions are about an organisation's responsibility to comply with the UK GDPR and how to demonstrate this compliance.

There are a number of measures organisations can, and in some cases must, take, for example doing a DPIA before any handling of information likely to result in a high risk to people. These include:

- data protection policies
- data protection by design and default
- data processor obligations and contracts
- data protection impact assessments (DPIAs)
- documentation (eg, a record of processing activities – RoPA)

- recording personal data breaches (PDBs)
- data protection officers
- codes of conduct and certification schemes

A full list of these measures is found in our guidance.

Data protection by design and default

This is concerned with privacy by design and is an integral element of being accountable.

Organisations are explicitly required to incorporate data protection by design and default into their processing. This means they should consider privacy and DP issues at the design phase of any system, and then throughout its lifecycle. DP should be embedded in their systems from the very beginning.

The DUAA also inserts a new provision on 'children's higher protection matters' into article 25 of the UK GDPR (data protection by design and by default). This requires online services likely to be used by children to consider children's needs, and how to design measures to protect and support child users into their service.

The organisation should begin by asking certain key questions such as:

- what is the risk to the people of the proposed processing?
- what should it do to comply with the principles and protect people's rights?

The key considerations are the same as those for security measures and include:

- available technology ('state of the art');
- the cost of implementation; and
- the risk to the rights and freedoms of people.

So again we come back to the importance of the information risk assessment.

The organisation should consider what internal policies and measures it should have in place to embed DP into its systems.

This is crucial at the design stage; before an organisation implements a system or buys a service, it must ask itself whether the system can support all its privacy requirements.

Its considerations could include:

- minimising the processing of personal information;
- pseudonymising personal information;
- ensuring transparency of handling; and
- creating and improving security measures.

So, security is key!

Example - a council wants to set up a new system of data sharing between social workers and other services

- A council wants to set up a new system of data sharing between services, eg social workers, who work with vulnerable children.
- The parties identify the minimal amount of personal information they will need to share and process to make the system effective and clarify whether they will be joint or separate controllers.
- The council completes an information risk assessment to ensure that the information is protected with appropriate security measures, for example pseudonymisation.
- The services discuss people's rights and what people will be told about the use of their information in the privacy notice.
- If the handling involves a high risk, this will involve a data protection impact assessment or DPIA and we'll discuss these next; but if the processing involves a low risk, they might have a checklist to make sure it addresses the basic data protection essentials.
- So in this way, the council implements a data sharing solution which embeds data protection into its design.

The Data Protection Impact Assessment (DPIA)

A DPIA is another essential accountability tool.

It helps the organisation to analyse its processing and identify and minimise DP risks.

A DPIA is required for any new processing which is likely to result in a high risk to the rights and freedoms of people.

For example, the UK GDPR requires a DPIA when an organisation plans to:

- use systematic and extensive profiling or automated decision making to make significant decisions about people;
- process special category data or criminal offence data on a large scale; or

- systematically monitor a publicly accessible place on a large scale.

We also require a DPIA if the organisation plans to:

- match data or combine datasets from different sources; or
- process personal data that could result in a risk of physical harm in the event of a security breach.

Our guidance contains a more complete list of handling where we require a DPIA.

What kind of information should be included in a DPIA?

Our guidance says organisations should do a DPIA should before their use of data begins, and should include the following steps:

- identify the need for a DPIA. As the council and services in the previous example are sharing information and combining datasets about vulnerable children, these operations are on our list as likely to result in high risk and so a DPIA is required;
- so, in the DPIA, the council should describe the nature, scope, context and purpose of its proposed handling;
- it should outline its consultation process with all the parties concerned;
- it must assess the necessity and proportionality of the processing and its compliance measures, including the lawful basis and how to support people's rights; and
- assess the risk of the processing and identify the measures taken to reduce any risks to people.
- If the council cannot take steps to successfully mitigate against this risk, then it must consult the ICO.

This will all be done with the advice of the council's Data Protection Officer (DPO) who will sign off and record outcomes.

There is a DPIA template on our website to help organisations.

Our role

If the DPIA finds that the processing poses a high risk to data subjects and if the risks of that processing cannot be successfully mitigated, the organisation must submit its DPIA to us.

We'll then either:

- provide the organisation with our view as to whether the measures proposed in the DPIA to mitigate that risk are adequate;

- provide advice how the organisation could mitigate any high risks;

  or

- we might advise the organisation not to use the information because it would be in breach of the UK GDPR.

And in rare circumstances, we might:

- issue a formal warning or take action to ban the use of information altogether.

Recording personal data breaches (PDBs)

A personal data breach (PDB) can be broadly defined as a security incident which has affected the confidentiality, integrity, or availability of personal data. So, there will be a PDB whenever any personal data is:

- accidentally lost, destroyed, corrupted, or disclosed;
- if someone accesses it or passes it on without proper authorisation; or
- if the data is rendered unavailable and this unavailability has a significant negative effect on individuals.

For example, sending personal data to the wrong recipient or a malicious attack which results in the loss of data.

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

Reporting a personal data breach

As part of their accountability obligations, controllers must notify us of any PDB within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of data subjects.

Data processors must inform controllers of any personal data breach and the controller should report the breach.

Regardless of whether or not a breach needs to be notified to us, the controller must keep documentation of all breaches. This should include any remedial action taken or the reasons why it decided a breach wasn't reportable.

Example – reporting a personal data breach

Let's take an example of a hospital which suffers a breach resulting in the accidental disclosure of patient records:

- there is likely to be a significant impact on the affected people;
- because the data is sensitive and confidential;

- this is likely to result in a high risk to their rights and freedoms; and
- so they would need to be informed about the breach without undue delay; and
- we need to be informed without undue delay and within 72 hours.

Informing people of a personal data breach

People should be informed if the breach is likely to result in a high risk to their rights and freedoms

They don't need to be informed, for example, if:

- the data is encrypted and unintelligible;
- steps have been taken to mitigate any risk; or
- it would involve disproportionate effort to contact people, perhaps where their contact details have been lost as a result of the breach.

In these circumstances, it may be appropriate for an organisation to communicate that a breach has occurred, for example by posting on their website.

Documentation

As part of its accountability obligations, each controller must maintain a record of processing activities (known as a RoPA). This is referred to as documentation.

It includes information such as:

- the purposes of the handling;
- a description of the categories of people and of the categories of personal information;
- retention schedules for the data; and,
- where possible, a general description of the technical and organisational security measures.

A data processor must also keep a record but not as much as the controller.

There are template RoPAs for the controller and processor on our website.

Documentation for organisations which employ fewer than 250 people

The requirement to maintain a RoPA is obligatory for controllers that employ 250 or more staff.

The UK GDPR provides a limited exemption for small and medium-sized organisations.

If the organisation employs fewer than 250 people, it need only document processing activities that:

- are likely to result in a risk to the rights and freedoms of individuals;
- aren't occasional (for example, are more than just a one-off occurrence and not something it does rarely); or
- involve special category data or criminal conviction and offence data.

The Data Protection Officer (DPO)

Article 37 outlines the requirement for some controllers and processors to appoint a data protection officer.

The UK GDPR sets out three specific circumstances in which an organisation must appoint a DPO. Only one of these has to be met for the obligation to apply:

- handling information which involves regular and systematic monitoring of data subjects on a large scale;
- a public authority (except for courts acting in their judicial capacity); or
- conducting large scale processing of special categories of data or criminal offence data.

A DPO's tasks include:

- informing and advising the organisation about its obligations to comply with the UK GDPR;
- being the first point of contact for us and people;
- providing training to staff; and
- advising on DPIAs and conducting internal audits.

The organisation can appoint a contractor or an existing member of staff to the role so long as they have the required experience and there won't be a conflict of interest with their other duties.

A single DPO can act for a group of companies or public authorities.

A DPO must be independent and can't be dismissed or penalised for doing their duties or because an organisation doesn't like what they've said.

Codes of conduct

A code of conduct is a voluntary tool that's intended to help the organisation comply with the UK GDPR.

They can be drawn up by trade associations or sector-specific representative bodies.

They're intended to provide compliance guidelines and set standards for best practice for that sector and should identify and address data protection issues that are important to the organisations concerned.

This might address issues such as fair and transparent handling or the exercise of people's rights.

Responsibility for monitoring the code lies with an independent 'monitoring body' unless the organisation is a public authority as this has its own internal monitoring mechanisms.

We must approve the code and the monitoring body.

Uptake is voluntary but we encourage it.

Certification

Certification is another voluntary means for an organisation to demonstrate that it's complying with the UK GDPR.

It involves the setting up of data protection certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance.

The certification scheme criteria can cover a specific issue like a security measure, or it can be more general like lawfulness of processing.

We approve the criteria.

Once an accredited certification body has assessed and approved an organisation, it'll issue them with a certificate, and a seal or mark relevant to that scheme.

Again, the uptake and use of certification is voluntary, but we encourage and support it.

The security and accountability obligations of the data processor

A data processor acts on the instructions of a controller. The processor can be an organisation or individual (such as a sole trader or self-employed professional).

A data processor has security and accountability obligations and constraints on what it can do.

Article 28 stipulates that handling by the data processor shall be governed by a contract. It outlines the information which must be provided in the contract, such as the categories of people, the types of information, and the nature and purpose of the handling.

Back to top

Optional further reading

Our website

In the Guide to the UK GDPR have a look at the section 'security'.

Read the 'At a glance' points and the 'In brief' questions and answers. In particular look at these specific questions:

- What does the UK GDPR say about security?
- What level of security is required?
- Should we use pseudonymisation and encryption?
- What are 'confidentiality, integrity, availability and resilience?'

Find an example in the guidance where an organisation's backup policy helps it to recover lost data after a ransomware attack (see the yellow boxes for examples).

In the Guide to the UK GDPR also have a look at the section 'accountability and governance'.

Read the 'At a glance' points and the 'In brief' questions and answers. In particular look at these specific questions:

- What is accountability?
- Why is accountability important?
- What do we need to do?

Don't forget to look at the ICO's sample DPIA Template and the Documentation Template for an organisation's Record of Processing Activities (RoPA).

Back to top

KNOWLEDGE SERVICES

UPDATED: 3 February 2026