# 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 7 of our data protection online training programme. These notes are not 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 and the relevant legislation open whilst watching the online module:

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

This document contains:

# Supporting notes

Module 7 looks at principle (f) and a controller's accountability and governance obligations. It covers:



## Principle (f) – integrity and confidentiality

This principle states that personal data shall be:

'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures'.

Principle (f) is concerned with the broad concept of information security. This includes cyber security and physical and organisational security.

Article 32 of the UK GDPR provides specifics about the security of processing.

This article states 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 controller to meet its key principle (f) obligation 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.

## Risk assessments, security policies and measures

The controller must consider the risk presented by the processing and use this to assess the level of security it needs to put in place.

It needs to think about the nature of the data and the consequences of losing it or of it being disclosed to the wrong people.

Recital 75 lists the type of data which is considered to be high risk. It includes special category data and criminal offence data.

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

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

The kinds of policies a controller 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 controller 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.

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.

**Example: the ICO holds personal data about stakeholders, complainants and its employees**

- We use firewalls to secure our internet connections.
- We choose the most secure settings for our devices and software and keep them up to date.
- We control who has access to our data and services.
- We protect ourselves from viruses and other malware.
- We backup key data and systems to ensure resilience.

This is a very high level summary, but the ICO has thousands of other technical and organisational controls ranging from intrusion prevention systems to user awareness training.

## The accountability and governance provisions

These are concerned with the controller's responsibility to comply with the UK GDPR and to demonstrate this compliance.

Technical and organisational measures are required by principle (f) but are outlined as part of these obligations.

## Data protection by design and default

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

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

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

- what is the risk to the data subject of the proposed processing?
- what should it do to comply with the principles and protect individual 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 the data subjects.

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

The controller should consider what internal policies and measures it should have in place to embed data protection into its systems.

This is crucial at the design stage; before a controller 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 data;
- pseudonymising personal data;
- ensuring transparency of processing; and
- creating and improving security measures.

Security is key!

**Example: a council wants to set up a new system of data sharing between social workers and other services such as the police and schools.**

- The council consults with the interested parties and they identify the minimal data they will need to share.
- They clarify whether they will be joint controllers or separate controllers for the data.
- They agree to pseudonymise third party personal data.
- The council completes an information risk assessment. It might also complete a data protection impact assessment or DPIA and we will discuss these next.
- The services discuss how to address the information rights of the data subjects.
- If the processing is low-risk, the council might have a checklist to make sure it addresses the basic data protection essentials. For example, it might:
    - update a privacy notice or put one in place; or
    - have a contract in place if they are using a processor.
- So in this way, the council implements a data sharing solution which embeds data protection into its design. Both the checklist and DPIA are part of this process.
- The council will also need to ensure its documentation is up to date.
- It may put in place a Data Sharing Agreement, as best practice in these situations.

## The Data Protection Impact Assessment (DPIA)

A DPIA is another essential accountability tool.

It helps the controller to analyse its processing and identify and minimise data protection risks.

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

For example, the UK GDPR requires a DPIA when a controller 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.

The ICO also requires a DPIA if the controller 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 processing where the ICO requires a DPIA.

## What kind of information should be included in a DPIA?

- a description of the nature, scope, context and purposes of each element of the proposed processing;
- any consultation with relevant stakeholders;
- an assessment of the necessity and proportionality of the processing in relation to the purpose and proposed compliance measures;
- an assessment of the risks to data subjects' rights and freedoms; and
- the measures in place to address risk (including security measures).

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

## The role of the ICO

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 controller must submit its DPIA to the ICO.

The ICO will then either:

- provide the controller with its view as to whether the measures proposed in the DPIA to mitigate that risk are adequate;
- provide advice how the controller could mitigate any high risks; or
- it might advise the controller not to carry out the processing because it would be in breach of the UK GDPR.

And in rare circumstances, it might:

- issue a formal warning or take action to ban the processing altogether.

**Example: a council is setting up a new system of data sharing between social workers and other services such as the police and schools.**

- They are sharing data about vulnerable children and are processing personal data that could result in a high risk. They are also combining datasets from a variety of sources.
- For these reasons a DPIA is required.
- The council must describe the processing and outline the nature, scope, context and purpose of each element.
- 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.

- This involves considering the lawful basis for the processing , ensuring data quality and minimisation, thinking about privacy information and how to support individual rights.

- Finally the DPIA must assess the risk of the processing and identify the measures taken to reduce any risks to data subjects.

- This will all be done with the advice of the council's Data Protection Officer.

## 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 processing;
- a description of the categories of data subjects and of the categories of personal data;
- retention schedules for the data;
- 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 record of processing activities 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 controller 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;
- are not 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.

**Example: an insurance company has 100 staff**

- It regularly processes personal data in the context of processing claims and sales. It should document this processing because it is not occasional but is regular.
- It occasionally carries out an internal staff engagement survey. It should not keep documentation for this.
- it occasionally collects information on applicants' health and ethnic origin for equal opportunities monitoring. It should keep documentation for this processing because it involves special category data.
- it occasionally does profiling on its customer database for the purposes of insurance-risk classification. It should keep documentation for this processing because profiling is intrusive and therefore constitutes 'risky' processing.

**Example: a council employs 800 members of staff**

- It must document its processing for all its processing activities.
- It regularly processes personal data when collecting council tax data and documents this processing activity.
- It occasionally carries out an internal staff engagement survey and also documents this, even though it is occasional.

- It collects information on employees' health and ethnic origin for equal opportunities monitoring. It should keep documentation for this processing whether it is regular or occasional.

- It designs a new system for sharing the personal data of vulnerable children with outside agencies and this processing must be documented.

## 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:

- processing data 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

- carrying out large scale processing of special categories of data or criminal offence data.

## A DPO's job description

Their tasks include:

- informing and advising the organisation about its obligations to comply with the UK GDPR;
- being the first point of contact for the ICO and data subjects;
- 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 cannot 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 is intended to help the controller comply with the legislation.

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

They are 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 processing or the exercise of people's rights.

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

The ICO must approve the code and the monitoring body.

Uptake is voluntary but encouraged by the ICO. The idea is to improve transparency and accountability.

## Certification

Certification is another voluntary means for a controller to demonstrate that it is 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.

The criteria are approved by the ICO.

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

The uptake and use of certification is voluntary but encouraged and supported by the ICO.

## Personal data breach

A personal data breach can be broadly defined as a security incident which has affected the confidentiality, integrity or availability of personal data. So there will be a personal data breach 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.

## Reporting a personal data breach to the ICO

As part of their accountability obligations, controllers must notify the ICO of any personal data breach 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 the ICO, 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. Controllers are encouraged to keep an internal register of all breaches.

## Informing data subjects of a personal data breach

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

They do not 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 individuals, perhaps where their contact details have been lost as a result of the breach.

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

**Example: a hospital suffers a breach resulting in the accidental disclosure of patient records**

- There is likely to be a significant impact on the affected individuals 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.
- The ICO needs to be informed without undue delay and within 72 hours.

**Example: a university experiences a breach where a member of staff accidentally deletes a record of alumni contact details**

- These details are subsequently reconstituted from a backup.
- This is unlikely to result in a high risk to the rights and freedoms of those individuals.
- The ICO does not need to be informed about the breach.
- The individuals do not need to be informed.
- The university should make a record of the breach even though it was not reported.

## The security and accountability obligations of the data processor

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

A 'processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

Article 28 states that a processor:

- shall not engage another processor without prior specific or general written authorisation of the controller;
- shall not process data except on instructions from the controller, unless required to do so by UK law;
- shall inform the controller of a personal data breach without delay;
- must set up technical and organisational measures to ensure a level of security appropriate to the risk, appoint a Data Protection Officer and assist the controller in responding to requests exercising the rights of data subjects; and
- must keep a record of processing if it employs more than 250 people.

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

**Back to top**

## Further reading

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 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?

The page 'For organisations' has a link to the ICO's Accountability Framework which is intended to help organisations meet and demonstrate their accountability obligations.

Now look at the following sections on the left under 'accountability and governance' and read the 'At a glance' points and one or two 'In brief' questions and answers for each one.

- Contracts
- Documentation
- Data protection by design and default
- Data protection impact assessments
- Data protection officers
- Codes of conduct
- Certification
- Personal data breaches

Don’t forget to look at the ICO’s sample DPIA Template and the Documentation Template for a controller’s Record of Processing Activities (RoPA).

Also accessible via the page ‘For organisations’ is the ICO’s Data Sharing Information Hub which provides guidance and practical tools for organisations on how to share data lawfully.

**Back to top**

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022