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

Introduction

These notes are designed to set out the key points covered during module 1 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 open whilst watching the online module.

This document contains:

Supporting notes

Module 1 gives a broad overview of the UK's data protection legislation and later modules will give more detail about the individual topics. This module covers:

The legislation

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) were both amended on 31 December 2020. This was to make them work as UK law, now that EU law no longer applies in the UK. You can find the correct up-to-date text on legislation.gov.uk:

- The UK GDPR
- The DPA
- The Privacy and Electronic Communications Regulations 2003 (PECR)

The UK GDPR is our version of the EU's GDPR. It contains 99 Articles and 173 Recitals. The articles are legally binding and form the backbone of our data protection legislation. The recitals are separate and give context to the articles. They are advisory only but make a useful starting point if you are unsure what an article means.

The DPA contains extra UK provisions.

Although the UK GDPR is very similar to the EU GDPR, make sure you always check the UK text on www.legislation.gov.uk, as there are some differences.

You should also always make sure you check the latest version of the DPA on www.legislation.gov.uk, as there are some changes from the original printed version.

The two pieces of legislation need to be read together and aren't complete as standalone documents.

You may also come across 'Keeling Schedules'. The government produced these during the Brexit transition period, to show what the new UK version of the law would look like with all the amendments. However, these weren't official legal texts. Now the amendments are in force, we should refer to the official updated text on www.legislation.gov.uk instead.

PECR covers electronic marketing including phone calls, emails and texts.

Key definitions

Personal data is any information relating to an identified or identifiable living person - also known as the data subject. For example, your date of birth and your badge number are your personal data and you are the data subject because this data relates to you.

The controller is the organisation responsible for the processing of the data. The ICO is a controller for the personal data it holds about you.

The controller may outsource its processing to another organisation who processes the data on its behalf. The processor can only process the data according to the instructions of the controller. For example, as a controller, the ICO outsources our payroll to another company. That company is a data processor which processes the data on behalf of the ICO.

The principles

The UK GDPR is based around 7 principles of information handling. An organisation must comply with these principles of processing.

They are listed in Article 5(1) and in summary they state that data shall be:

(a) processed lawfully, fairly and in a transparent manner;
(b) collected for specified, explicit and legitimate purposes – this is known as purpose limitation;
(c) adequate, relevant and limited to what is necessary – this is known as data minimisation;
(d) accurate and, where necessary, kept up to date;
(e) kept for no longer than is necessary for the identified purposes – this is known as storage limitation; and
(f) processed in a secure manner using appropriate technical or organisational measures.

There's a final accountability principle at Article 5(2) which states that the controller shall be responsible for, and be able to demonstrate compliance

with, the listed principles. The controller is expected to keep documentation to meet this requirement.

Example: the principles in practice

I join a gym and provide it with my personal data.

- It must ensure the data it holds is accurate and secure.
- It must only collect data for the purposes it has identified and must not further process it for incompatible purposes. For example, the gym must not give my data to a third party who might want to send me emails about fitness holidays.
- The gym should also ensure it is not collecting more data than is necessary for processing my membership. Remember this is called data minimisation.

- The gym must have a clear retention policy which specifies for how long it will keep my data.
- Finally, the processing must always be fair and within my reasonable expectations. The gym must be transparent about its processing and should provide me with information about what it is doing with my data in a privacy notice. It should also record this information in its own documentation.

If it meets all these requirements the gym should be in compliance with the data protection principles.

Lawful bases for processing

The first principle at Article 5(1)(a) states that processing must be lawful, fair and transparent. The requirement for lawfulness takes us to Article 6 because, in order to be lawful, processing must be based on an Article 6 basis for processing.

The first is lawful basis (a) where consent to the processing has been provided.

The others state that processing is necessary for:

(b) The performance of a contract.
This applies when your employer processes your data in order to pay you.

(c) Compliance with a legal obligation.
For example, the ICO has a legal obligation to give our salary details to HMRC for tax purposes.

(d) The protection of vital interests where the processing is a matter of life and death.
For example, a hospital processing data for an unconscious victim of a traffic accident.

(e) The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
This applies when the council processes your council tax details.

(f) The purposes of the legitimate interests pursued by the controller or by a third party.
These interests must be weighed against the interests and rights of the data subject, so this basis involves some judgement, and a balancing test called a legitimate interests assessment or LIA.

Example: lawful bases for processing

In order to process my membership, the gym wants to ask me for my address and bank details. It wants to ask for my fitness goals and to track how often I attend.

- It must identify which Article 6 bases for processing are relevant to each of these processing activities.
- It might process my bank details and address because we have entered into a contract.
- It might hold my fitness goals because it has my consent.
- It might consider it has a legitimate interest in processing data about my attendance.
- It performs an LIA to balance its interests against my interests and rights and it concludes this processing is likely to be within my reasonable expectations and is unlikely to be of any detriment to me.

Special category data

Special categories of data are listed in Article 9 of the UK GDPR. These categories are data concerning:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data when used for identification purposes;
- Health data (physical or mental); and
- Data concerning an individual's sexual life or orientation.

Because this data is by its nature more sensitive than ordinary data, it is given extra protection, and processing special category data is prohibited unless certain conditions are met.

There are ten conditions for processing special category data listed in Article 9 and further conditions are found in Schedule 1 of the DPA.

For example, there's a condition which says processing is allowed if the data subject has given their explicit consent to that processing. The controller must obtain an expressed statement of consent from the individual.

Example: processing special category data

My gym now wants to ask me for data about my health.

- Remember a controller must always have an Article 6 lawful basis for processing. In these circumstances, this is consent.
- Because health data is special category data, the gym will also need an Article 9 condition for processing.
- The most appropriate condition is explicit consent.
- The gym membership form has a section which explicitly states I agree to it processing my health details should I require medical help. I sign it to clearly signal my agreement.
- In this example, there's a clear link between the Article 6 lawful basis (consent) and the Article 9 condition for processing (explicit consent) but this is not always the case with the other special category conditions.

Article 10 Criminal offence data

Article 10 sets out separate safeguards for personal data classed as criminal offence data.

This is personal data relating to criminal convictions and offences or related security measures. It also includes allegations about offences.

Under Article 10, processing may be carried out either :

- under the control of official authority
  (for example, the DVLA has authority to process personal data about speeding fines);

  or

- when it is authorised by UK law (this appears as 'domestic law' in the UK GDPR, but in all cases this means 'UK law' and so throughout the modules the term 'UK law' has been used).

As with Article 9, this means when certain conditions for processing are met.

For example, there's a condition which says processing is allowed if it is necessary for the prevention or detection of a crime.

These conditions are found in the DPA – this is a good example where the UK GDPR and the DPA need to be read together.

Example: processing criminal offence data

I break into someone's car in my gym car park and it has CCTV footage showing me committing this crime.

- The gym passes this data to the police. It considers it has a legitimate interest to do so and this provides its Article 6 basis for processing.
- However because the data relates to a crime, the gym must meet the requirements of Article 10.
- It does not have official authority to process criminal offence data and so needs authorisation in UK law which means a condition for processing.
- There's a condition for processing in Schedule 1 of the DPA which allows processing for the prevention or detection of a crime.
- The gym must consider whether processing is necessary for this purpose, but if so, it may rely upon this condition.
- Remember if it is lawful, the processing is in compliance with principle (a) which states processing must be lawful, fair and transparent.

Individual rights

The UK GDPR also accords the individual specific rights with respect to their personal data:

- The right to be informed (to be told, for example, what data is held and the purpose of the processing, the recipients of the data and how long it will be stored for);
- The right to be given access (this is known as the subject access right and we talk about people making a data SAR or DSAR. This is commonly called a SAR);
- The right to rectification (which means to have data corrected);
- The right to erasure (otherwise known as the right to be forgotten);

- The right to restriction of processing (where processing is suspended, for example, while a request for rectification is considered);
- The right to data portability (this means the right to have data transferred in a common reusable format. For example, data might be transferred between two energy providers);
- The right to object to processing (including direct marketing); and
- The right not to be subject to a decision based solely on automated processing, including profiling. This applies only if that decision produces legal effects concerning the individual or similarly affects them.

I might make a SAR to my gym to request all the data it holds about me. I might ask it to rectify the data it holds – for example if it has made a mistake and recorded the wrong post code, I can ask it to correct this data.

Exemptions

An exemption can affect or restrict the application of the UK GDPR provisions.

If an exemption applies, a controller may not have to comply with all the usual rights and obligations such as:

- the right to be informed;
- the right of access; or
- the obligation to comply with the principles, for example the obligation to be transparent about processing.

The exemptions are listed in the DPA and this is another example where the UK GDPR and the DPA need to be read together.

Example: exemptions

The gym has passed the CCTV footage of me breaking into a car to the police. Unaware of this,

- I make a subject access request for details of the data it holds and ask whether it has passed my data to a third party.
- Usually you would expect the gym to tell me if it has passed my data to someone else. But if it tells me it has given CCTV footage of me to the police, I might disappear.
- Giving me this information would be likely to prejudice the police investigation.
- In this situation, the gym can apply an exemption which allows it to withhold data if its disclosure would be likely to prejudice the detection of a crime.
- In response to my SAR, it provides me with my personal data but it does not tell me it has passed CCTV data relating to me to the police.
- I remain unaware and am arrested the next day.

Law Enforcement processing

Part 3 of the DPA covers certain processing of personal data by competent authorities for the purposes of law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

This applies to the police as a competent authority processing for law enforcement purposes.

Part 3 is a standalone part of the DPA and it has its own principles and rights, and its own bases and conditions for processing.

For example, once the police receive the CCTV footage of me breaking into a car, they are processing for law enforcement purposes under Part 3.

Intelligence Services processing

Intelligence Services processing is covered in Part 4 of the DPA.

It applies to processing by MI5, the Secret Intelligence Service (also known as MI6), GCHQ and data processors acting on their behalf. Like Part 3, Part 4 stands alone and is complete in itself.

For example, if MI5 are collecting intelligence about me at the gym, their processing falls under Part 4.

The role of the ICO

The ICO is responsible for monitoring and enforcing the application of our data protection legislation.

The UK GDPR lays out the tasks and powers of the ICO, and Article 57 lists tasks such as:

- to promote awareness of controllers and processors of their data protection obligations; and
- to handle and investigate complaints lodged by a data subject.

Article 58 lists the ICO's powers, such as the power:

- to carry out audits;
- to impose an administrative fine; and
- to approve draft codes of conduct.

Further details concerning the Information Commissioner are outlined in Part 5 and Schedule 12 of the DPA.

The Information Commissioner

Schedule 12 of the DPA includes the Commissioner's appointment by the Crown for a term not exceeding seven years. In practice, initially the Commissioner is usually offered a term of five years.

And notice we are independent of government – we are a regulator and strictly not part of the civil service.

Part 5 of the DPA includes the UK functions the Commissioner must fulfil - such as:

- reporting to Parliament;
- preparing codes of practice;
- powers of audit; and
- fees which may be charged.

Enforcement powers

There are different ways for us to promote compliance with the UK GDPR:

- we educate organisations by publishing guidance and providing advice;
- we deal with complaints informally by getting organisations to change their behaviour; and
- we take formal enforcement action in more serious cases.

The Commissioner's enforcement powers

These are covered in Part 6 of the DPA.

Information notices require a controller or processor to provide the Commissioner with information when we are investigating their compliance.

Assessment notices require a controller or processor to permit the Commissioner to carry out a compulsory audit. An audit is an assessment of whether the organisation is in compliance with the data protection legislation.

Enforcement notices enable the Commissioner to order steps which must be taken by a controller or processor when it has failed to comply with the legislation. For example, if it hasn't complied with the UK GDPR principles.

We also have **powers of entry and inspection** – we have the ability to apply to a court for the issue of warrants – for example where a controller has committed an offence under the UK GDPR or PECR and we wish to enter an office to seize the computers or files.

We can also issue administrative fines (known as **Monetary Penalty Notices**) for serious compliance failures.

In addition, the Commissioner has the power to prosecute for criminal offences.

These include the unauthorised viewing or trading of data. This is one of the most frequent offences we see where, for example, someone who works in a hospital might look at another person's medical records without any authorisation.

Another key offence is deliberately destroying personal data which has been requested.

There's also an offence which applies to us. Section 132 of the DPA prohibits disclosure of information by ICO staff (unless the disclosure is made with lawful authority). It's really important to note this because we have access to some very sensitive data working at the ICO and it's crucial we understand the sensitivity of this data and don't disclose it to anyone outside the organisation.

The Privacy and Electronic Communications Regulations 2003 (PECR)

PECR covers an area where there's real potential to impinge on an individual's privacy because it covers nuisance phone calls and electronic marketing.

There are two distinct parts to PECR:

Part 1 covers the non-marketing requirements of PECR - the rules mainly concerning data capture in relation to telecoms such as telephone calls and the internet.

Part 2 covers direct marketing by electronic means (for example, marketing by phone, email and text).

We receive lots of complaints about direct marketing and it's worth noting here that Article 21(2) of the GDPR gives individuals the absolute right to object to processing for direct marketing purposes, including profiling.

PECR only applies to unsolicited electronic marketing, and any direct marketing by post falls under the UK GDPR.

Back to top

Further reading

Go to the homepage of the ICO website.

Note that there's a section called 'Your data matters' for individuals and a section called 'For organisations'.

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

Go to the Guide to the UK GDPR, take a look at the index on the left:

Key definitions
Principles
Lawful basis for processing
Individual rights

Follow some of these links and get a feel for how the guidance is structured with the key questions it asks. Explore some of the links to other resources.

Now go back to the homepage of the ICO website and this time click on the link 'For organisations'.

This also has links to the legislation we regulate but it lists other resources and support.

On the left follow the link to the Guide to LE Processing and have a look at the structure of this guidance for law enforcement processing.

Return to the 'For organisations' page and have a quick look at the Children's Code hub, titled 'Children's code: additional resources'.

This introduces the Age Appropriate Design Code which is an example of a Code of Practice we have prepared.

Have a look at the Enforcement pages by following the link 'Action we've taken' and 'Enforcement Action'.

Back to top

KNOWLEDGE SERVICES
UPDATED: 06 MAY 2022