Data Protection and PECR Training

Supporting notes and further reading

Module 6 : Principles part 2 – purpose limitation, data minimisation, accuracy and storage limitation

Introduction

These notes are designed to set out the key points covered during module 6 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
- ➢ Further reading

Supporting notes

Module 6 looks at four Article 5 principles of processing. It covers:

Principle (b) – purpose limitation

The purpose limitation principle can be split into two main requirements.

Data must be:

- collected for specified, explicit and legitimate purposes; and
- not further processed in a manner that is incompatible with those purposes.

Specified, explicit and legitimate purposes means:

- The controller has to specify the purposes of the processing at the time the data is collected.
- The data subject has a right to be informed about the purpose of the processing. This information should be provided in the privacy information provided by the controller.

Not further processed in a manner that is incompatible means:

- The controller has to consider whether any further uses of personal data are incompatible with the original purposes the data was obtained for.

- The purposes do not need to be exactly the same, but they must be not incompatible with the original purpose.

- If a controller's purposes change over time or it has a new purpose which it did not originally anticipate, it may not need a new lawful basis as long as the new purpose is compatible with the original purpose.

- This does not apply to processing based on consent. Consent must always be specific and informed, and re-using the data for a new purpose would unfairly undermine the original consent. A controller would usually need to get fresh consent which specifically covered the new purpose.

Example: processing which is not incompatible with the original purpose

- A gym monitors the attendance of its members.

- It processes this data on the basis of legitimate interests, and it informs new members about this processing in its privacy notice.

- The gym considers it has a legitimate interest in processing this data and so this provides its Article 6 lawful basis.

- It now decides it wants to start sending emails to members who haven't attended for a while, outlining classes they may be interested in.

- This processing is not incompatible with the original purpose and may be done on the basis of legitimate interests.

- It's worth pointing out that if the member does not want these emails, they do have the right to object.

Example: processing for a new purpose which requires consent to be renewed

- A company which is part of the energy network holds a register of vulnerable customers.
- The register identifies individuals who may have medical conditions or age-related requirements which mean their energy service needs to be prioritised.
- They have collected this data on the basis of consent.
- They now want to share it with water companies and think they have a legitimate interest for this disclosure.
- However if the energy company has been relying on consent, it will need to get fresh consent to specifically cover the new purpose.
- In this situation we would also recommend new privacy information and a Data Protection Impact Assessment. This is because it is high-risk processing of special category data on a large scale.

Other important points about purpose limitation:

- Under Article 30, controllers should specify their purpose for processing as part of the requirement to document the processing they carry out. This is a record of processing activities – referred to as a RoPA.
- The principle also says that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purpose(s).
    - The processing must be subject to appropriate safeguards which ensure that technical and organisational measures are in place, in particular in order to ensure respect for the principle of data minimisation.
    - These measures could include pseudonymisation.

The data quality principles

The principles of data minimisation, accuracy and storage retention set standards for the **'quality'** of personal data.

A controller's data should be of a good quality and not used to the detriment of the individuals concerned.

It is also important to be aware that the principles interconnect. This means that failure to comply with one of the principles can lead to problems with the others.

Controllers should regularly check the quality of the personal data they hold. They should correct any inaccurate records, remove irrelevant ones and update any which are out-of-date.

It may not always be practicable for a controller to check the quality of every record it holds, but it should at least be possible to check a sample. A controller needs to ensure it remains compliant – it cannot assume it remains compliant because it once was.

This is closely linked to principle (a) and the fairness of processing.

Example: how the data quality principles are related

- a company holds the addresses of all its customers.
- It does not regularly review its records to check how old they are.
- It may find that over time, it is holding a lot of data which is not adequate for the purpose for which it was collected because it is inaccurate.
- The data is excessive and has been kept for longer than is necessary.
- This infringes all three data quality principles – accuracy, data minimisation and storage retention.

Principle (c) – data minimisation

There are three parts to principle (c) – data must be:

1. adequate;
2. relevant; and
3. limited to what is necessary in relation to the purposes for which it is processed.

The UK GDPR does not define these terms – it depends on the circumstances of each case. The purpose for processing is the key factor - a controller will not be able to judge any of these points unless it is clear about why it is holding and using the data.

The controller must strike a balance:

- Why does it need the data?
- Does it hold too much? If so, it is likely to be excessive and irrelevant.

For personal data to be adequate, controllers should ensure that they process enough data to fulfil the purposes they are processing for, but not more than this.

Information should be sufficient to fulfil its purpose(s) in relation to the individual concerned.

Examples: data which is not adequate for the purpose

- A doctor deciding what treatment to give a patient needs all the medical information about them for that specific purpose. Any less would be inadequate.

- A shop CCTV system that produces poor quality images that can’t identify shoplifters is inadequate for the purpose.

The level of information a controller requires may vary from one data subject to another, depending on the purpose of the processing – data that is relevant for some people may be excessive when held about others.

Example: is the data relevant?

- A company asks every new recruit for a copy of their driving licence and details of driving convictions.
- Whether this is excessive will depend on the purpose for processing the information.
- If the organisation has some staff who drop off deliveries by van and other staff who only do administration work, the company doesn't need to hold driving licence details for everyone - just the group of people who do the driving.
- The company should be able to justify why it needs to have all the separate pieces of personal data about each person. Information should not be held 'just in case' it might be useful at some point in the future.

Example: is the data relevant?

- A gym asks a new member for a copy of their medical records.
- It may need to know some medical information, for example, details of any conditions that could affect the member's ability to use the gym.
- But it's unlikely that the gym would need a full copy of the member's medical records. They should only ask the individual for relevant information.

Example: is the data relevant?

- A bank asks a new customer for their current address and any addresses they have lived at in the last 20 years.
- It is reasonable to request a current address but 20 years of address history is unlikely to be relevant and limited to what is necessary.
- The bank may need more than a current address – it may need address details for the last three or five years to verify identity, or to comply with other laws such as those to prevent money laundering.
- They would need to be able to justify why it was asking for this information going back 20 years.

There are two parts to principle (d) but both parts interlink – this is because if information is not kept up to date, it is likely that it will become inaccurate.

This principle looks straightforward. However, it is not practical for a controller to check accuracy every time it uses the data or to constantly update it. For example, it wouldn't be reasonable to expect a bank to phone customers to check their addresses each time it sends out a letter or statement.

The DPA gives a definition of inaccurate - in relation to personal data it means incorrect or misleading as to any matter of fact.

The definition is particularly useful in casework where a complainant is arguing about the accuracy of data held about them – it can be difficult where opinions differ as to what is fact.

For example, the minutes of a meeting state a participant lost their temper and shouted at the others. The individual argues they did not lose their temper and did not shout. They say this is a matter of fact and want the minutes changed. In cases such as these, we would argue that if the *facts* of the matter cannot be objectively ascertained, both *opinions* should be recorded in a supplementary statement which should be added to the file. In this case, the statement would be added to the minutes.

Article 16 covers the right to rectification of inaccurate personal data and supplementary statements.

Example: accuracy and supplementary statements

- A doctor makes a misdiagnosis when recording that she thinks a patient has appendicitis.
- She also records she thinks the patient is depressed.
- In both cases, the medical record accurately reflects what the doctor thought at the time.
- The patient might argue they were not depressed and that this note on their medical record should be removed – in these circumstances, a supplementary note would be added to the file.
- In this example, although the medical record contains information about the diagnosis which is strictly 'incorrect', it does not infringe principle (d).

Principle (d) states that every reasonable step must be taken to ensure that personal data which is inaccurate is erased or rectified without delay.

When deciding what steps would be reasonable, controllers should have regard to the purposes for which the data is processed.

The more important the information, the greater the effort the controller should make to verify its accuracy. For example, a HR department processing job applications for a teacher would need verification of their teaching qualifications but would have less need to check details about a summer job from twenty years ago.

The second part of principle (d) says that data must be accurate and where necessary kept up-to-date. The UK GDPR doesn't define 'necessary' – the controller must make a judgement based on the purposes for which the information is being processed.

Records may contain information that is no longer 'correct' without infringing principle (d). For example, a record that someone was pursued for a debt which was subsequently found they do not owe, is likely to be held as a record demonstrating why particular actions were taken at the time.

Example: keeping personal data up-to-date

- A company delivers a one-off order to a customer.
- It keeps the address details for a certain period for accounting purposes and in case of complaints, but doesn't need to post anything else out to the individual.
- It will ask again for an address if another order is received.
- In this case it won't be necessary for the company to keep the customer's address details up to date.
- If the same company gives its staff a pay rise every April, there is an obvious need for staff payroll details to be updated and accurate.

Principle (e) – storage limitation

Principle (e) states that personal data shall be:

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data is processed.

- The UK GDPR does not set out any maximum or minimum retention periods for personal data.

- This is because we consider the controller is in the best position to judge how long it needs to retain information.

- In order to ensure fair and transparent processing in accordance with the right to be informed, a controller must provide individuals with details about the retention of their data in its privacy information. So it should know what its retention period will be when it collects the data.

- It should ensure that the retention period is limited to a strict minimum and should set time periods for a periodic review of the data, to consider whether it should be erased or de-identified. This should be laid out in its retention policy.

When deciding how long to retain personal data, a controller should consider:

- Any statutory requirement to retain information – for example, schools and hospitals have legal requirements to keep data for a specific amount of time;

- Industry guidelines or standards;

- The value of the information;

- The risks of retaining the information;

- The need to keep the information accurate and up to date.

Finally, personal data may be stored for longer periods if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Where this is the case, appropriate safeguards must be in place.

Retaining personal data for longer than necessary does not comply with principle (e), but there are also other risks:

- The controller has the responsibility of keeping data it doesn't need secure.

- It could also mean more work in responding to a data request.

- Keeping too much data could also infringe principles (c) data minimisation and (d) accuracy.

- If the data goes out of date, the wrong information could be used in error and the more time passes the more difficult it may be to ensure the accuracy of the information.

- Information that is kept for longer than necessary is also likely to be irrelevant and not limited to what is necessary.

The controller must take care not to delete or de-identify the data too soon, as it may risk infringing principle (c) adequacy.

Example: retention and the data quality principles when a relationship between controller and data subject ends

- The ICO keeps HR records about each of its employees.

- It makes a decision about the minimum data it must hold.

- The data must be accurate and adequate for the purposes identified. For example, the ICO must pay us the right amount and monitor our sick leave.

- If an employee leaves, the ICO will not need to keep all the data it holds about that individual.

- It doesn’t need to keep all their performance reviews. But it will be necessary to keep enough information to provide references for that employee, or for pension purposes.

- When a relationship between a controller and data subject ends, it doesn’t always mean the controller will need to delete all the personal data it holds for that individual. It may still have a need to retain certain information.

Back to top

Further reading

In the Guide to the UK GDPR have a look at the four sections in turn:

1. purpose limitation
2. data minimisation
3. accuracy
4. storage limitation

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

1. Purpose limitation:

- How do we specify our purposes?
- Once we collect personal data for a specified purpose, can we use it for other purposes?'

Find an example in the guidance where data is processed for purposes which are incompatible with the original purposes for which it was obtained (see the yellow boxes for examples).

2. Data minimisation:

- How do we decide what is adequate, relevant and limited?
- What about the adequacy and relevance of opinions?

Find examples in the guidance which describe situations where an organisation might hold data which is irrelevant and excessive (see the yellow boxes for examples).

3. Accuracy:

- When is personal data 'accurate' or 'inaccurate'?
- What about accuracy of opinions?

Find examples in the guidance which describe situations where incorrect data should be retained by organisations (see the yellow boxes for examples).

4. Storage limitation

- Do we need a retention policy?
- What should we do with personal data that we no longer need?

Find examples in the guidance which describe how organisations assess for how long they need to keep the personal data they hold (see the yellow boxes for examples).

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022