Data Protection and PECR Training

Supporting notes and further reading

Module 2 : Definitions

Introduction

These notes are designed to set out the key points covered during module 2 of our data protection online training programme. They 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 2 discusses key data protection definitions found in Article 4 of the UK GDPR and Part 1 of the DPA. These are:

- ➢ Personal data

Personal data

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

A deceased person is not a data subject and data relating to them does not fall under the data protection legislation.

In many cases it is clear – there is no doubt that data 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 data? and
- does the data relate to an identifiable person?

In most cases the data will obviously be about an individual who can be identified from it.

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

The question of a photograph is less clear. Whether a photo of me is personal data will depend on the nature of the picture:

- Am I identifiable from the photo?
- Is the image linked to my name?
- Am I the focus of the photo?

If people are incidentally captured in an image and are clearly not the focus of the image (for example, a busy street scene) – the image is unlikely to be personal data.

Other examples include:

- My manager's opinion of me in a performance review.
- The valuation of my house for the assessment of my council tax.
- A complaint about my work. This will be my personal data because it relates to me but it will also be the personal data of the complainant.
- My car registration number in the hands of the ICO. There is no means of knowing I own a particular car by looking at the registration number alone. As the ICO can look up a registration number and see that the car is mine, this number becomes my personal data in the hands of the controller.

  In this case, the controller has used other information it has access to, to identify who an individual is. It must also bear in mind that other individuals might hold information which means an individual can be identified.

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

In some circumstances, data may not be personal data – 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 individual in post), the salary information about the job is personal data 'relating to' that employee.

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

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

Data concerning a sole trader is personal data but data concerning a limited company is not.

Example: Personal data 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 data held in complaints files.

- Imagine an individual 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 individual 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 data.
- The details of the complaint itself will be the complainant's personal data.
- Any disciplinary steps taken against the nurse as a result of the complaint would not be the personal data of the complainant.
- A note on the file explaining that the complainant was removed from the premises because of threatening behaviour is that individual's personal data 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 individual and so won't be personal data at all.
- So in this situation, the controller must identify the personal data and decide who the data subject is for each piece of information.

Example: Personal data 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 data of identifiable individuals.
- 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 individual's personal data.
- The employee's opinion about a new project is their personal data.
- 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 data.

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 data subject is deceased then the Access to Health Records legislation applies rather than data protection legislation.

Example: Personal data in a photograph

- We need to consider the context of the personal data and this is relevant when thinking about a picture of a crowd at a football match.
- In this example, the purpose of the photograph and its processing is relevant.
- If a crowd of people at a football match are photographed by a journalist, the individuals caught in the photo are not its focus.

- It is not intended that the photograph will be used to learn or decide anything about them. It is therefore not personal data.
- However if one of the crowd members is recognised by a work colleague who then sends the photograph to their employer to prove that the person is not sick, the employer will be processing the photograph as personal data.
- The context of the data is really important.

Please see the guidance to personal data for further explanation and more useful examples.

Pseudonymisation and anonymisation

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

The definition of pseudonymisation is:

"The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information".

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 data has been anonymised.

Pseudonymisation is largely a security measure and pseudonymised data remains personal data.

Data which falls under the data protection legislation

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

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

A filing system is any structured set of personal data 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 data intended to form part of a filing system. This means that data 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 controller holds what we call manual unstructured data – 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 data - unless the controller is a public authority. For example, the contents of my ICO locker are definitely unstructured!

If manual data is not structured and it is held by a public authority, different conditions apply because a public authority is subject to the Freedom of Information Act 2000.

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

Processing

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

- collection
- organisation
- storage
- retrieval
- use
- dissemination
- restriction
- destruction
- recording
- structuring
- adaptation or alteration
- consultation
- disclosure by transmission
- alignment or combination
- erasure

Data sharing counts as disclosure.

Storage (simply holding the data) counts as processing.

A controller therefore doesn't have to be actively doing anything with the data for it to be caught under the definition of processing.

The personal data breach

A personal data breach is a breach of security leading to:

- accidental or unlawful destruction,
- data loss or alteration,
- unauthorised disclosure, or
- unauthorised access

...to personal data transmitted, stored or otherwise processed.

It's not simply a question of the disclosure or loss of personal data.

Example: 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 data 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 controller to consider whether the breach should be reported to the ICO. For example, we have internal procedures in place for circumstances where a caseworker sends data to the wrong organisation.

The controller should notify the ICO of any personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons.

Data processors must also inform controllers of any breach.

Health and social work professional, recipient, accuracy

Part 7 section 204 in the DPA gives miscellaneous UK-specific definitions including a health professional and social work professional.

Schedule 3 of the DPA gives other useful definitions which concern the processing of:

- Health data
- Social work data
- Education data and
- Child abuse data

A recipient is defined in Article 4 of the UK GDPR as a natural or legal person, public authority, agency or another body to which the personal data are disclosed. This is relevant in the context of data sharing.

The DPA also defines inaccurate (in Part 7 Section 205) and explains that in relation to personal data, it means incorrect or misleading as to any matter of fact.

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 data.

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

For example, the ICO is a controller and processes our personal data. It may send out our payroll details to be processed by another company and that other company is a data processor who processes the data on behalf of the ICO. But it is 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 database to send the mailing out and record any responses.

- In these circumstances, the council is a controller because it is determining the purpose for which the data is being processed and the means of the processing.

- The private company is a data processor because it is processing the data on behalf of the council (and following the council's clear instructions). It is not 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 data 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 controllers who share personal data might remain as separate controllers if they process the data for different purposes.

Back to top

Further reading

In the Guide to the UK GDPR have a look at the section 'What is personal data'. Read the 'In brief' questions and answers.

Then follow the link 'In more detail'. Choose four of these questions and read the explanations to help consolidate your learning.

Find an example in the guidance of a company pseudonymising the personal data it holds (see the yellow boxes for examples).

Find an example in the guidance where the purpose of the processing is relevant to the question of whether data is personal data.

Now go back to page Guide to the UK GDPR and this time click on the link 'Controllers and processors'. Read the 'At a glance' and 'Checklists'.

Again, click on the 'In more detail' and read the sections 'How do you determine whether you are a controller or processor' and 'How does this apply in practice'.

Find some examples of processing which illustrate whether an organisation is a controller or processor in practice.

The guidance on contracts between a controller and processor also contains useful information.

Optional further reading

Personal data breaches are discussed in the guidance however we will talk further about these in another module.

Also see the FOI guidance 'Access to information held in complaint files' .

There is further useful information in the detailed SAR guidance under the heading 'Are there any special cases: unstructured manual records'.

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022