Data Protection and PECR Training

Supporting notes and further reading

Module 12: DPA Part 3

Introduction

These notes are designed to set out the key points covered during module 12 (Part 3) of our data protection online training programme. 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 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 12 session 1 covers law enforcement processing by competent authorities under Part 3 of the DPA. It covers:

Introduction: Part 3 DPA

Part 3 of the DPA covers processing for criminal law enforcement purposes by competent authorities such as the Police.

It implements the European Law Enforcement Directive (known as the LED) into UK law. A directive provides more flexibility than a regulation and has to be transposed into a country's domestic law before becoming legally binding. It's more suitable for law enforcement purposes as each country will do this slightly differently, and so in practice each country will implement the LED in a different way.

In contrast, an EU regulation such as the EU GDPR requires the text to be implemented by all member states in its entirety, meaning it is exactly the same across all the EU countries. The UK GDPR currently reflects the EU GDPR (but may deviate in time).

Article 2 of the UK GDPR explicitly says that it doesn't apply to the processing of personal data for law enforcement purposes.

Law enforcement purposes

Part 3 applies to information which is processed for law enforcement purposes by a competent authority. Section 31 of the DPA lists these purposes, which are:

- the prevention, investigation, detection or prosecution of **criminal** offences;

- the execution of **criminal** penalties; and

- safeguarding against, and prevention of, threats to public security.

This **doesn't** cover **civil enforcement processing** which falls under the UK GDPR.

We've now published guidance for organisations sharing data with law enforcement authorities: Data sharing information hub | Sharing personal data with law enforcement authorities. An organisation may process data under the UK GDPR and then pass it onto the police who will then process it under Part 3 of the DPA. For example, the processing of data by banks for the purposes of detecting crime, such as fraud, initially falls under the UK GDPR. If they pass fraud data to the Police or National Crime Agency, these competent authorities will process it under Part 3.

An organisation such as the police won't process all the personal data it holds for law enforcement purposes. For example, they're likely to process general HR data under the UK GDPR. Law enforcement organisations will therefore process data under both pieces of legislation. We've also published useful guidance about: Data sharing information hub | Data sharing and the reuse of data by competent authorities for non-law enforcement purposes.

Competent authorities

Section 30 of the DPA defines a competent authority as:

a) a person specified in Schedule 7 of the DPA; and

b) any other person that has statutory functions for any of the law enforcement purposes.

Schedule 7 of the DPA gives a list which covers:

- the UK government ministerial departments;
- chief officers of police and other policing bodies;
- other authorities with investigatory functions;
- authorities with functions relating to offender management; and
- other authorities (eg the director of Public Prosecutions, the ICO).

This list may be amended by a statutory instrument (please see Statutory Instruments - UK Parliament for a helpful explanation of statutory instruments).

The intelligence services aren't listed as competent authorities as they're governed by the provisions in Part 4 of the DPA.

A competent authority also includes any other person that has statutory functions for any of the law enforcement purposes.

This means:

- any public authority with powers to investigate and/or prosecute crimes and impose sentences; or

- any other organisation empowered by law to exercise those powers in a way that gives them control over the data (as a controller, as opposed to a processor).

For example, this includes a local authority when prosecuting trading standards offences or the Environment Agency when prosecuting environmental offences.

In another module, we discussed a gym which collects CCTV footage to monitor its car park. This falls under the UK GDPR because the gym isn't a prosecuting authority or a law enforcement authority.

Remember that to fall under Part 3, the processing must be by a competent authority **and** for law enforcement purposes. Both requirements must be met.

Example: a police force processing under Part 3 and the UK GDPR

- The Police are investigating an individual they suspect of committing a burglary.

- The Police are a competent authority and are handling the individual's personal data for law enforcement purposes.

- This handling of personal data falls under Part 3 of the DPA.

- The officer in charge of the investigation does a good job and is promoted - the Police HR department record the officer's new pay grade and salary.

- This **isn't** processing for a law enforcement purpose and falls under the UK GDPR

Part 3 principles

We've seen that the handling of personal data under the UK GDPR must comply with the six data protection principles outlined in Article 5.

In the same way, processing under Part 3 must comply with its own principles. They mirror the UK GDPR principles (a) to (f) but are slightly different.

They are numbered 1 to 6 and have specific requirements regarding law enforcement processing. See sections 35 to 40 in Part 3 of the DPA.

- Principle 1 (lawful and fair).
- Principle 2 (purpose).
- Principle 3 (adequate, relevant and not excessive).
- Principle 4 (accuracy).
- Principle 5 (storage limitation).
- Principle 6 (security).

For example, principle 4 (accuracy) says that personal data based on facts must - so far as possible - be distinguished from personal data based on personal assessments. This means there must be a clear differentiation between subjective witness statements and factual evidence.

The requirement for accuracy doesn't apply to the content of a statement but to the fact that a specific statement has been made.

Intelligence information must be flagged, and not confused with provable, factual information.

The police must also clearly identify the person suspected of an offence, the victims and the witnesses.

Under principle 5, there should be a way for the data that's collected to be regularly reviewed so it's not retained for longer than is necessary.

Example: Part 3 principles in practice

- The Police interview all the witnesses to a crime and keep a record - they must only process this data for the specific law enforcement purpose they have powers to undertake and for which it was collected, such as investigating a criminal offence

- The Police must only record relevant data and not keep excessive information.

- The Police clearly identify the facts of the case and the witness statements.
- The Police clearly identify the person suspected of the offence, the victim and the witnesses.
- The Police keep the data securely and for their specified retention period.

Part 3 lawful processing

The first data protection principle says that processing for law enforcement purposes must be lawful and fair (section 35 in Part 3).

To be lawful, the handling of personal data must be based on law. This could cover a range of things, including statute, common law, royal prerogative or statutory code. It will depend on the specific laws to which the relevant competent authority is subject. Some authorities (like the police) may be able to rely more heavily on common law than other organisations which are more constrained by the nature of their constitution and legal framework.

In addition, the processing is lawful, if either –

- the data subject has given consent to the processing for that purpose; or
- processing is necessary for the performance of a task carried out for that purpose by a competent authority.

Remember that principle (a) of the UK GDPR requires processing to be lawful fair and transparent. Under Part 3 principle 1, there's no requirement for transparency. This is because there will be circumstances in which a law enforcement agency will need to be able to neither confirm nor deny that it's processing an individual's personal data. This could be because doing so would reveal operationally sensitive or potentially damaging information and could prejudice an ongoing criminal investigation.

Although it isn't defined here, the threshold for consent is equivalent to that required under the UK GDPR.

In practice, consent is often hard to obtain in law enforcement. This is because in many circumstances individuals may not have a genuine choice about the processing.

Part 3 sensitive processing

Principle 1 defines 'sensitive processing' and gives this processing extra protection (section 35). This is similar to special category data under the UK GDPR.

It concerns the processing of:

(a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
(c) data concerning health;
(d) data concerning an individual's sex life or sexual orientation.

Sensitive processing may be quite common in law enforcement given the types of scenarios and data collected.

Under section 35(3), sensitive processing is only permitted in two cases, if:

(a) the data subject has given consent, and
(b) the controller has an appropriate policy document (or APD) in place;

or

(a) the processing is strictly necessary for law enforcement purposes,
(b) the processing meets at least one of the conditions in Schedule 8,

and

(c) at the time when the processing is carried out, the controller has an APD in place.

Remember, the APD is a document which explains a controller's compliance with the principles and retention policies. This requirement is laid out in section 42 of Part 3.

You can read more about sensitive processing in our Guide to law enforcement | Conditions for sensitive processing, where there's also a link to a template APD for Part 3 processing.

Schedule 8 contains the conditions for sensitive processing under Part 3 and includes conditions such as statutory purposes, legal claims, judicial acts and preventing fraud.

Remember that in circumstances involving law enforcement processing, consent can be problematic and difficult to obtain.

Example: lawful processing under Part 3

- The Police are investigating a crime and handle the personal data of the suspect to see if they've committed other crimes.
- This is processing by a competent authority for law enforcement purposes and so falls under Part 3 of the DPA.
- The processing must be lawful and fair under principle 1 – there's no need to be transparent.
- The processing must be based on law and in this case, the Police also consider that processing is necessary for the performance of a task carried out for LE purposes – they don't want or need to ask for the individual's consent.
- In this situation, the Police can't process by consent because the individual would be likely to refuse consent if they thought it could prevent the investigation.
- There's no sensitive processing involved.

Example: sensitive processing under Part 3

- In this example, the Police are investigating a fight where the victim is badly injured.
- This is processing by a competent authority for law enforcement purposes and so falls under Part 3 of the DPA.
- The processing must be lawful and fair under principle 1 – it's based on law and processing is necessary for the performance of a task carried out for LE purposes by a competent authority.
- The Police don't want or need to ask for the consent of the individual to the processing.
- Because the charges involve the health of the victim, this involves sensitive processing.
- The Police consider the processing is necessary for law enforcement purposes and have an APD in place.
- They will also rely on the Schedule 8 condition paragraph 1 - statutory purposes.
- This says the condition is met if the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.

Individual rights

Part 3 Chapter 3 of the DPA gives the individual specific rights with respect to the processing of personal data for a law enforcement purpose.

These include:

- the right of access by the data subject, and
- the rights to rectification, erasure and restriction.

There's no right to data portability or to object to processing (including direct marketing).

A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. In practice, solely automated processing is rarely used in the law enforcement context and is unlikely to have any operational implications. There's often an element of human interaction involved, which means the processing isn't 'solely automated'.

For example, although a database of criminal records or prosecution histories is an automated processing system, it isn't automated decision making.

The information an individual is entitled to under the right of access is listed in section 45. This largely works in the same way as the UK GDPR right of access:

- a controller must also respond to any request exercising a right within a month. This cannot be extended.

- A controller might also refuse a manifestly unfounded or excessive request, or charge a reasonable fee.

Restricting a data subject's rights

A restriction works like an exemption and limits the rights a data subject might exercise.

If a controller wishes to restrict an individual's rights, it must tell them the reasons why their rights have been restricted.

This may not be applicable if giving this explanation would itself undermine the purpose of imposing the restriction - eg the Police may not want to tell an individual that they're under investigation.

The controller must also explain the right to:

- make a request to the Information Commissioner under section 51 of the DPA (to check processing is compliant with the DPA or that the refusal of a request is lawful);

- complain to the Information Commissioner; and

- apply to a court under section 167 of the DPA.

Restrictions to the Part 3 rights are relevant to the law enforcement purposes.

For example, there's a category of data called 'relevant data' which is contained in a judicial decision or in documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. If this data is processed in the course of a criminal investigation or proceedings, a controller doesn’t have to make information available or allow other rights relating to that data. This is because defendants will have access to such data through alternative routes, such as the court disclosure process.

In many cases, a controller may also restrict all or part of the right of access and/or the provision of information to the data subject, if this is a necessary and proportionate measure to:

- avoid obstructing an official or legal inquiry, investigation or procedure,
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,
- protect public security or national security, and
- protect the rights and freedoms of others.

In deciding whether restricting access is necessary and proportionate, a controller needs to consider the rights and legitimate interests of the data subject.

Finally, if personal data must be kept for the purposes of evidence, the controller shouldn’t rectify or erase it if requested, but should instead restrict its processing.

Our Guide to law enforcement | Individual rights explains in more detail how a controller might limit the provision of information with respect to each right.

Example: restricting the data subject’s rights

- An individual is recorded on CCTV breaking into a car. A passer-by stops them, but is then attacked by the individual. This is witnessed by a number of people.
- The individual thinks the CCTV footage has been disclosed to the Police and requests a copy from the Police.
- The individuals asks the Police to tell them what the Police are doing with this personal data and ask the Police to delete it. They ask for a full copy of any witness statements.

- The Police are interviewing witnesses and are about to press charges.

- The Police refuse to inform the individual about this processing because this would prejudice the prosecution of a criminal offence. They refuse to provide the witness statements because this would also prejudice the investigation and they also must protect the rights and freedoms of these other people. The Police also refuse to erase the CCTV footage because it contains evidence

- If the victim requested details of the Police's processing about the assault, the Police might not restrict their right to be informed in these circumstances. This is because this disclosure wouldn't prejudice the prosecution of the offence.

Controller and processor under Part 3

The terms controller and processor are defined in section 32 of the DPA.

A controller is a competent authority which, alone or jointly with others:

- determines the purposes and means of the processing of personal data, or
- has an obligation under an enactment to process data.

Only competent authorities can be joint controllers under Part 3.

Any arrangement between a controller which is a competent authority and one which isn't cannot be a joint controller arrangement. For example, this applies to arrangements between police counter-terrorism units and the intelligence services, because the intelligence services aren't competent authorities.

A processor is defined as:

- any person who processes personal data on behalf of the controller (other than a person who's acting as an employee).

Part 3 Chapter 4 makes provision for both controllers and processors:

- their general obligations;
- specific obligations with respect to security;
- obligations regarding personal data breaches; and
- data protection officers.

Whichever UK DP regime applies to the controller will also apply to its processors. So, if a processor is acting for a controller who's a competent authority processing for law enforcement purposes, the processor provisions found in Part 3 will apply – even if the processor itself isn't a competent authority.

Logging

In line with section 62 of the DPA, both controllers and processors have a requirement to log certain data – see Guide to law enforcement processing | Accountability and governance | Logging.

This applies to metadata for automated systems, for example, logs of any changes to the data, recording who made them and when.

This includes logs of the collection, alteration, consultation, disclosure, combination, and erasure of data.

The Police have automated systems like the police national computer (PNC) and the automatic number plate recognition (ANPR) system – each force will have their own.

Competent authorities must keep:

- logs of consultation (who consulted and when), and
- logs of disclosure (who disclosed, and the recipients).

Section 62 of the DPA lists the purposes the logs may be used for, for example, to verify the lawfulness of processing.

The controller or processor must also make the logs available to the Information Commissioner on request.

The transfer of data to third countries or other organisations

Part 3 Chapter 5 of the DPA deals with the transfer of personal data to third countries or international organisations.

It specifies that the transfer must meet certain conditions such as:

- it's necessary for a law enforcement purpose;

- it's based on an adequacy decision or there are appropriate safeguards;

- it's based on special circumstances (for example, to protect vital interests);

- the intended recipient is a relevant authority in a third country (a competent authority) or a relevant international organisation.

There are also provisions for transfers which aren't to a relevant authority.

Back to top

Further reading

Have a look at our Guide to law enforcement processing | Scope and key definitions.

Read the 'At a glance' points and the 'In brief' questions and answers:

- What is a competent authority?
- Are we processing for law enforcement purposes?
- What is sensitive processing?

Find an example of the Police processing data recorded on a body-worn camera (examples are in the yellow boxes).

In our Guide to law enforcement processing | conditions for sensitive processing, have a look at the following:

- What are the conditions?
- What is an appropriate policy document?

Have a look at our Guide to law enforcement processing | Individual rights and in particular the Right of Access.

Have a look at the section about logging.

Find an example of the Police using logging to help with an internal investigation.

Back to top

KNOWLEDGE SERVICES
UPDATED: 30 AUGUST 2022