Data Protection and PECR Training
Supporting notes and further reading
Module 5 : Processing criminal offence data

Introduction

These notes are designed to set out the key points covered during module 5 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 5 looks at processing criminal offence data. It covers:

Requirements of Article 10

Article 10 is concerned with the processing of personal data relating to criminal convictions and offences or related security measures.

Remember that processing for law enforcement purposes by competent authorities (for example, the Police) is separate to this and falls under Part 3 of the DPA.

So Article 10 covers processing of what we call criminal offence data by non-competent authorities.

In order to meet the requirements of Article 10, a controller must either

- process the data under the control of official authority; **or**
- seek authorisation for processing under UK law.

Article 10 also states:

Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 10: criminal offence data

Article 10 states that it covers the processing of personal data relating to criminal convictions and offences or related security measures.

Section 11 in Part 2 Chapter 2 of the DPA also states that Article 10 covers:

- the alleged commission of offences by the data subject; and
- proceedings for an offence committed or alleged to have been committed by the data subject, or the disposal of such proceedings, including sentencing.

So the DPA adds to the definition given in the UK GDPR.

We collectively refer to this as criminal offence data. This includes:

Data about a specific criminal conviction or trial, such as
- criminal activity;
- allegations;
- investigations; and
- proceedings.

Data relating to criminal convictions and offences, such as:
- unproven allegations; and
- information relating to the absence of convictions.

A wide range of related security measures, such as:
- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; and
- civil measures which may lead to a criminal penalty if not adhered to.

If this data is being processed for law enforcement purposes by a competent authority such as the Police, then the processing will fall under Part 3 of the DPA and not Article 10.

Example: my gym processing CCTV footage of me breaking into a car in the gym car park

- The gym processes this personal data of mine by disclosing it to the Police.
- The gym considers it has a legitimate interest in processing this data and so this provides its Article 6 lawful basis.
- Because this data concerns the allegation of an offence, as a non-competent authority processing criminal offence data, the gym must comply with Article 10.
- The Police will process the data under Part 3 of the DPA. This is because they are a competent authority processing the data for law enforcement purposes.

Example: a school employs a teacher following a clear criminal records check

- The school keeps this result in its personnel files.
- The data 'relates to' criminal convictions and so collecting and holding it means the school is processing criminal offence data.
- It must meet the requirements of Article 10 even though the check does not reveal any convictions.
- This is because the data relates to criminal convictions, even though there are none.

Article 10: under the control of official authority

- A controller may process criminal offence data if it has official authority.
- It may also keep a comprehensive register of criminal convictions only if it has official authority.

The key point is that 'official authority' must be laid down by law and the controller must be able to identify the specific law.

For example, the DVLA has a specific official authority to process any criminal offence data it holds, as well as to keep a comprehensive register of motoring offences.

But a public authority doesn't automatically have official authority to process criminal offence data.

Article 10: authorisation for processing under UK law

If a non-competent authority who does not have official authority wishes to process criminal offence data it must ensure the processing is authorised by UK law.

In the previous examples, this applied to both my gym and the school. They are not competent authorities and they do not have any official authority to process criminal offence data. They therefore need to identify authorisation in UK law for the processing.

Section 10 subsection 5 of the DPA says that processing meets the requirement in Article 10 of the UK GDPR for authorisation in UK law, only if it meets a condition for processing in Parts 1, 2 or 3 of Schedule 1.

Remember that Parts 1 and 2 contain the conditions we discussed with reference to Article 9 (special category data) and that there are 23 substantial public interest conditions in Part 2.

Now in addition to this, we have Part 3 conditions which relate specifically to Article 10 data.

Conditions for processing in Schedule 1, Parts 1 and 2

The Schedule 1, Parts 1 and 2 conditions for processing can be relied upon for the processing of both special category data and criminal offence data.

This means that if a controller is processing criminal offence data which is also special category data, it may be able to rely on the same condition for processing both sets.

The list of substantial public interest conditions in Part 2 is not exactly the same for criminal offence data as it is for special category data. You can see below there are some gaps. This is because some of the conditions apply only to special category data and **not** criminal offence data.

Schedule 1 Part 1 and 2 conditions

1. Employment, social security and social protection
2. Health or social care purposes
3. Public health
4. Research

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes

10. Preventing or detecting unlawful acts
11. Protecting the public against dishonesty
12. Regulatory requirements relating to unlawful acts and dishonesty
13. Journalism in connection with unlawful acts and dishonesty
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering

17. Counselling
18. Safeguarding of children and individuals at risk

23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

For example, paragraph 8 (the equality of opportunity condition we discussed in the last module) applies to special category data but **not** criminal offence data.

Conditions for processing in Schedule 1 Part 3

The Schedule 1 Part 3 conditions are specifically for criminal offence data.

Paragraphs 29-34 are conditions similar to the UK GDPR conditions for processing Article 9 data.

Instead of being listed in Article 10 of the UK GDPR, they are outlined in Schedule 1 Part 3 of the DPA.

This means there is further consistency in the conditions for Articles 9 and 10.

Schedule 1 Part 3 conditions

29. Consent
30. Vital interests
31. Not-for-profit bodies
32. Manifestly made public by the data subject
33. Legal claims
34. Judicial acts
35. Administration of accounts used in commission of indecency offences involving children

37. Insurance

Processing necessary for reasons of substantial public interest

As we have seen, the Schedule 1 Part 2 substantial public interest conditions apply both to criminal offence data and to special category

data processing. Each of these conditions outlines their own processing requirements.

Some of the conditions assume that processing under that condition is always in the substantial public interest, for example ensuring equality or preventing fraud. Other conditions explicitly require the controller to demonstrate that the processing is 'necessary for reasons of substantial public interest'.

This means the controller must explain why the specific processing is necessary for the public interest. This covers a wide range of values and principles relating to the public good, or what is in the best interests of society.

There are eleven paragraphs in Part 2 which have this requirement, including:

6. Statutory and government purposes
10. Preventing or detecting unlawful acts
17. Counselling
18. Safeguarding of children and individuals at risk

However, this only applies when the controller is processing special category data. It does not apply to criminal offence data because of Schedule 1 paragraph 36 which changes the way these conditions work.

This means that when relying on one of the relevant eleven paragraphs in Schedule 1 Part 2, a controller does **not** have to explicitly demonstrate that the processing is 'necessary for reasons of substantial public interest' when processing criminal offence data.

This is because it is assumed that if a controller is processing criminal offence data for one of the reasons listed in the conditions, it is always going to be for reasons of substantial public interest in order to protect the public from crime, and so there's no need to outline the arguments.

The requirement generally remains in place for the processing of special category data because these conditions do not assume that processing special category data is always in the public interest.

So if the controller is processing special category data, it must outline its substantial public interest arguments, if required to do so by the condition. Remember, not all the conditions have this requirement.

The controller should do this in its documentation.

We can see that the substantial public interest conditions in Schedule 1 Part 2 do not work in the same way for criminal offence data as they do for special category data. There is a table in the guidance listing the conditions which require the controller to demonstrate the substantial public interest when processing special category data.

Statutory and government purposes: processing necessary for reasons of substantial public interest

Schedule 1 Part 2 paragraph 6 provides a condition for processing for statutory and government purposes, where those purposes involve the exercise of a function.

This condition is met if the processing:

(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, **and**
(c) **is necessary for reasons of substantial public interest**.

Remember in the last module, we looked at an example for the Health and Safety Executive (HSE). We saw that subsection (1)(b) of the condition states the processing must be necessary for reasons of substantial public interest.

In our example, the HSE was processing special category data and so had to explain why the processing was necessary for reasons of substantial public interest.

This would not be necessary if the HSE was processing criminal offence data.

Preventing or detecting unlawful acts: processing necessary for reasons of substantial public interest

This was the condition for processing my gym used when it passed CCTV footage of me committing a crime in its car park to the Police: it relied on paragraph 10 for the disclosure.

This condition is met if the processing:

(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, **and**
(c) **is necessary for reasons of substantial public interest**.

At sub paragraph 1(c), the condition explicitly requires the controller to demonstrate that the processing is 'necessary for reasons of substantial public interest'.

However, as we have seen, this particular requirement does **not** apply to criminal offence data. So taking the example of my gym, it can rely on this condition, but does **not** have to explain the public interest in disclosing the CCTV footage of the crime to the Police.

Example: my gym passes CCTV footage of me to the Police

- The gym considers it has a legitimate interest to process this data and so this provides its Article 6 lawful basis for processing.
- 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 or a condition for processing in Schedule 1.
- As we have seen, paragraph 10 in Schedule 1 Part 2 of the DPA allows processing for the prevention or detection of an unlawful act.
- But because this is criminal offence data, there is no requirement to explain the substantial public interest in the disclosure.

The role of consent

Given the risks to individuals, there is more emphasis on obtaining consent for processing criminal offence data (and special category data).

Some of the conditions require the controller to justify why it cannot give individuals a choice and get consent for the processing.

Even where it is required, the law acknowledges there may be good reasons why a controller cannot get valid consent in some cases.

So in the previous example, paragraph 10 allows the gym to disclose my data to the Police without asking for my consent, because to do so would alert me to the trouble I was in, and prejudice the detection of the crime. See subparagraph 1(b) in paragraph 10 above.

There is a list in the guidance which shows which conditions require the controller to justify why consent for the processing was not obtained from the data subject.

Example: a school keeps records of clear criminal record checks

- The school has a legal obligation to process this data so this provides its Article 6 lawful basis for the processing.
- The data 'relates to' criminal convictions and so collecting and holding it means the school is processing criminal offence data.
- It is not a competent authority processing for law enforcement purposes and so must meet the requirements of Article 10.
- It does not have 'official authority' to process this data and so needs authorisation in UK law or a condition for processing in Schedule 1.
- As it has a legal obligation under employment law to conduct DBS checks, the school can rely on paragraph 1 – the employment condition.

Example: the DVLA processing motoring offences

- The DVLA has official authority to process criminal offence data and to keep a comprehensive register of motoring offences.
- Its Article 6 lawful basis might be the exercise of official authority vested in the controller.
- Because it is processing criminal offence data, it must meet the requirements of Article 10.
- In these circumstances, because it has official authority to process this data, it does **not** need a condition for processing.

The Appropriate Policy Document (APD)

An appropriate policy document is a short document outlining a controller's compliance measures and retention policies for special category and criminal offence data. An APD is required by almost all of

the substantial public interest conditions (and also for the employment, social security and social protection condition).

In its APD, a controller should briefly outline:

- the Schedule 1 condition (or conditions) it is relying on;
- its procedures for complying with each of the principles;
- its retention and deletion policies; and
- an indication of the retention period for the specific data.

The ICO has produced an APD template to help controllers meet this requirement. There are links to this template in the guidance.

The guidance also contains a table showing the conditions which require an APD.

Back to top

Further reading

In the Guide to the UK GDPR have a look at the section 'criminal offence data'.

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

At the bottom of the page click on the link to take you to the detailed guidance on criminal offence data. You should take some time to read these paragraphs but in particular, look at:

- 'What are related security measures?'

On the left, now click on 'What are the rules on criminal offence data?'

And read the sections:

- What does 'under the control of official authority' mean?
- What counts as a 'comprehensive register' of criminal convictions?
- When is processing authorised by UK law?

Find an example of an employer who is keeping a 'blocklist' of individuals with criminal convictions who work in their industry. Is the company in compliance with Article 10? (See the yellow boxes for examples).

Also follow the link on the left: 'What are the conditions for processing?'.

And read the sections:

- What conditions are available?
- Are the conditions the same as for special category data?
- How do the other conditions work? (Note the useful table!)
- Do we need to show 'substantial public interest'?
- What does 'necessary' mean?
- How does consent work?
- Do we need an 'appropriate policy document'?

Find an example where a delivery company wants to perform a criminal record check on its self-employed riders. Which condition for processing might it apply to this processing? Why can't it rely on consent? (See the yellow boxes for examples).

In particular look at the useful table showing which Schedule 1 conditions require the controller to justify why it has not obtained consent for its

processing, and also which conditions require an appropriate policy document (APD).

Don’t forget to look at our appropriate policy document template.

The ICO’s APD shows you what one might look like in practice.

Back to top

KNOWLEDGE SERVICES
UPDATED: 29 APRIL 2022