Data Protection and PECR Training
Supporting notes and further reading
Module 12: DPA Part 4

Introduction

These notes are designed to set out the key points covered during module 12 (Part 4) 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

Module 12 session 2 covers intelligence services processing under Part 4 of the DPA. It covers:

Introduction: Part 4 DPA

Part 4 of the DPA sets out a specific, tailored data protection regime for:

- the intelligence services, and
- their processors.

This is separate from general processing under the UK GDPR or Part 3 of the DPA, and is based on an international data protection standard to which the UK is a signatory signatory (the Council of Europe's Modernised Convention on the Protection of Personal Data (Convention 108+)).

Unlike the UK GDPR or the LED, Part 4 of the DPA doesn't derive from EU legislation because the EU isn't 'competent' in matters of national security and so can't dictate how member states approach these matters.

The intelligence services

Part 4 covers processing by the:

- Security Service (sometimes called MI5);
- Secret Intelligence Service (sometimes called SIS or MI6);
- Government Communications Headquarters (GCHQ); and
- processors acting on their behalf.

These are collectively known as 'the intelligence services'.

Part 4 of the DPA covers the handling of personal data by the intelligence services and their processors **for any purpose** – eg including HR and payroll processing.

Not all provisions of Part 4 of the DPA were in place at the time the DPA came into force. This was to give the intelligence agencies time to prepare. These provisions were enacted into law in 2019 by Statutory Instrument and include provisions about the right to be informed and general obligations of controllers. See DPA Changes to legislation.

Part 4 of the DPA provides its own definitions, principles and data subject rights relating to intelligence services processing.

The DPA gives:

- conditions for processing under Part 4 of the DPA in Schedule 9;
- conditions for sensitive processing in Schedule 10; and
- other exemptions in Schedule 11.

Part 4 principles

There are six intelligence services principles which are similar to the UK GDPR and Part 3 principles:

- Principle 1 (Lawful, fair and transparent)
- Principle 2 (Purpose)
- Principle 3 (Adequate, relevant and not excessive)
- Principle 4 (Accuracy)
- Principle 5 (Storage limitation)
- Principle 6 (Security)

For Part 4 of the DPA processing, principle 1 says it must be lawful fair and transparent. Under Part 3 principle 1, there's no requirement for transparency - so this is a key difference.

Please see our Guide to intelligence services processing | Principles for more information.

Part 4 lawful processing

Principle 1 says that to be lawful under Part 4 of the DPA, the processing must meet at least one of the conditions in Schedule 9 of the DPA and, in the case of sensitive processing, at least one of the conditions in Schedule 10.

Schedule 9 of the DPA includes six conditions for processing:

- consent;
- contract;
- legal obligation;
- vital interests;
- public functions; and
- legitimate interests.

Schedule 10 of the DPA includes nine conditions for sensitive processing:

- consent to particular processing;
- right or obligation relating to employment;
- vital interests of a person;
- safeguarding children and of individuals at risk;
- data already published by the data subject;
- legal proceedings etc;
- administration of justice, parliamentary, statutory etc and government purposes;
- medical purposes; and
- equality.

There's no exemption from the principle 1 requirement for the processing to be lawful, even if the national security exemption is applied.

Part 4 sensitive processing

This concerns the sensitive processing of:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
- genetic data for the purpose of uniquely identifying an individual,
- biometric data for the purpose of uniquely identifying an individual,

- data concerning health,
- data concerning an individual's sex life or sexual orientation,

plus:

- the commission or alleged commission of an offence by an individual, and
- proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

The data is similar to special category data and criminal offence data under the UK GDPR.

Please see our Guide to intelligence services processing | Scope and key definitions | What is sensitive processing? for more information.

Individual rights

Part 4 of the DPA includes the following individual rights:

- to information (eg the identity of the controller and the legal basis for the processing);
- of access – a controller can charge a fee for a SAR under Part 4 of the DPA – the maximum fee is set at £10;
- to object;
- to rectification;
- to erasure;

plus the right:

- not to be subject to automated decision-making;
- to intervene in automated decision-making; and
- to information about decision-making.

Controllers should communicate any information they're required to provide by Part 4 of the DPA in clear and plain language.

These rights may be refused if an exemption applies to the processing.

An individual can also exercise their rights by making a complaint to us or by taking matters to court.

There's more detail about this in our Guide to intelligence services processing | Individual rights.

Obligations

Controllers have a responsibility to ensure their compliance with the provisions of Part 4 of the DPA, and to be able to demonstrate this to us.

Controllers must consider the impact of their processing on individuals, and implement measures to ensure they comply with the principles and minimise the risks to individuals' rights and freedoms.

Controllers and their processors must implement appropriate security measures.

Controllers must report serious personal data breaches to us – a personal data breach is serious if it seriously interferes with individuals' rights and freedoms.

Personal data may only be transferred outside the UK if this is necessary and proportionate for the controller's statutory functions or certain statutory purposes.

Processors must undertake to the controller to:

- implement appropriate measures to ensure that processing complies with Part 4 of the DPA; and
- provide information to the controller to demonstrate compliance.

Processors don't have the same obligations or responsibility as controllers – but processors do have some direct obligations of their own under Part 4 of the DPA (eg they must inform the controller without undue delay if they become aware of a personal data breach).

There's more information in our Guide to intelligence services processing | Obligations.

The national security exemption

This is a wide-ranging exemption in section 110 of Part 4 of the DPA.

It can exempt the handling of personal data from the data protection principles and the rights of individuals.

It can also exempt processing with respect to:

- personal data breach reporting; and
- some of the powers of the Information Commissioner including the Information Commissioner's notices and powers of entry and inspection.

There's no exemption from the principle 1 requirement for the processing to be lawful. Controllers must also still comply with their general accountability and security obligations.

The national security exemption is available for controllers to apply when they consider that's reasonably necessary to safeguard national security. This isn't a blanket exemption. Controllers should be able to show on a case-by-case basis that compliance would raise a real possibility of an adverse effect on national security.

There's no specific definition of what's meant by national security, but it's generally understood to cover the security and well-being of the UK as a whole, its population, and its institutions and system of government. For example, it can cover protection against specific threats, such as from domestic or international terrorists or hostile states.

There's further information in our Guide to intelligence services processing | Exemptions.

National Security Certificates

National Security Certificates are covered in the DPA sections 111 and 130 of the DPA 2018.

A Minister of the Crown can issue a certificate which covers the processing.

If a controller applies the national security exemption, the existence of an applicable certificate is conclusive proof that the exemption applies in the circumstances described in the certificate (and so we can't rule that it was was applied incorrectly).

The national security exemption can still apply without a national security certificate.

If a certificate has been issued, the controller doesn't have to rely on it and can still decide to comply with the request and not apply the exemption, should they choose to. It's at their discretion.

We publish details of relevant certificates on our website.

You can find more information in our Guide to intelligence services processing | Exemptions | What are national security certificates?.

Other exemptions

There are other exemptions in Schedule 11 of the DPA. These include, for example, exemptions for:

- parliamentary privilege, and
- the economic well-being of the UK.

Please see our Guide to intelligence services processing | Exemptions | Are there any other exemptions? for more information.

Finally, when working with personal data related to the intelligence services, some will be marked as 'Secret' and 'Top Secret'. This means specific rules relating to the Government Security Classifications will apply.

Example: an individual who works as a spy makes a SAR to their employer, the Secret Intelligence Service

- The individual requests all the personal data SIS holds about them and pays £10.
- SIS explain they can have a copy of part of their employment record but other parts are exempt.
- The request falls under Part 4 of the DPA and the individual has a right of access under section 94 of the DPA.
- The withheld information is exempt under the national security exemption.
- It's marked as TOP SECRET in the file and cannot be disclosed - this is part of the Government Security Classification scheme.
- There may also be no requirement to tell the individual that information has been withheld (or any other rights haven't been actioned due to the exemption) if that would cause the sort of difficulty the exemption is there to avoid.
- The controller must respond promptly and within a month.

Back to top

Further reading

Exemptions

Have a look at our Guide to intelligence services processing | Scope and key definitions.

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

- What is Part 4?
- Who is covered by Part 4?
- What are controllers and processors?
- What about other key definitions?
- What is sensitive processing?
- Who is not covered by Part 4?

In our Guide to intelligence services processing | Principles, have a look at What is the first principle?

Have a look at our Guide to intelligence services processing | Individual rights, particularly the Right of Access.

Have a look at our Guide to intelligence services processing | Exemptions and read about the national security exemption.

Find an example where an intelligence service applies the national security exemption in response to a SAR (the examples are in the yellow boxes).

Look at the sections which explain how the other exemptions in Schedule 11 of the DPA work. Find an example where an intelligence service applies the negotiations exemption.

Back to top

KNOWLEDGE SERVICES
UPDATED: 30 AUGUST 2022