

About the Guide to Intelligence Services Processing	2
Scope and key definitions	3
Principles	7
Individual rights	14
Obligations	21
Exemptions	26

About the Guide to Intelligence Services Processing

The Guide to Intelligence Services Processing is part of our [Guide to Data Protection](#). It is for those who have day-to-day responsibility for data protection in the intelligence services.

It explains the data protection regime that applies to the intelligence services. It covers Part 4 of the Data Protection Act 2018 (DPA), which is separate from the UK GDPR regime.

It explains each of the data protection principles, rights, obligations and exemptions. It summarises the key points you need to know and answers frequently asked questions.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance.

This section only covers processing by the intelligence services. If you are not one of the intelligence services, you need to read our [Guide to the UK GDPR](#) or [Guide to Law Enforcement Processing](#).

Scope and key definitions

At a glance

- The intelligence services, and those processing personal data on their behalf, are not subject to the UK GDPR or the law enforcement provisions of the DPA.
- Instead, they must comply with Part 4 of the DPA, which sets out a separate data protection regime for intelligence services processing.
- A controller is defined as the intelligence service who determines how and why the data is processed. Processors process data on their behalf, but may share some accountability for the processing.
- There are additional rules which apply to "sensitive processing" of some specified types of particularly sensitive data.
- This guidance is only directly relevant to the intelligence services (and processors acting on their behalf). Other organisations processing for national security purposes must comply with either [Part 3 of the DPA](#) (if a competent authority), or the [UK GDPR](#).

In brief

- [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?](#)

What is Part 4?

Part 4 of the DPA sets out a specific, tailored data protection regime for the intelligence services and their processors. This is separate from the general processing regime (UK GDPR) or the law enforcement processing regime (Part 3).

The data protection principles, standards and obligations provided for in Part 4 have been drafted to reflect and ensure consistency with the standards in the Council of Europe's Modernised Convention on the Protection of Personal Data (Convention 108+). Convention 108+ has been signed by numerous countries worldwide, including the UK.

This guidance will help you to understand who Part 4 applies to, and how it is different to the UK GDPR or the law enforcement provisions.

Further Reading

[Key provisions in the DPA 2018 - see Part 4, Chapters 1-6](#)

External link

Who is covered by Part 4?

Part 4 only applies to the three specified intelligence services:

- the Security Service (MI5);
- the Secret Intelligence Service (SIS); and
- the Government Communications Headquarters (GCHQ).

These are collectively known as “the intelligence services”.

If you are one of these intelligence services, or a body which is part of these services such as the National Cyber Security Centre (which is part of GCHQ), then **all** processing of personal data you undertake is governed by Part 4 of the DPA.

Part 4 also covers processors acting on behalf of one of the intelligence services.

It covers processing of personal data for **any purpose**, by the intelligence services and those processing on their behalf.

What are controllers and processors?

The definitions of “controller” and “processor” are contained in section 83. A controller is defined as the intelligence service which determines the purpose and means of the processing. A processor is defined as a person (other than an employee) who processes personal data on behalf of the controller. These definitions are essentially the same as for the UK GDPR. For more information, see our [UK GDPR guidance on identifying the controller](#). The obligations of [controllers](#) and [processors](#) are set out in sections 102-106.

Two or more intelligence services can operate as joint controllers when they jointly determine the purposes and means of processing. But please note that the intelligence services can only enter into a joint controller relationship with each other. Intelligence services cannot be in a joint controllership relationship with a controller which is not itself an intelligence service processing under Part 4.

If you are a processor acting on the instructions of one of the intelligence services, you need to comply with the processor obligations in Part 4. See [‘What obligations do processors have?’](#)

Example

A company processes payroll data for an intelligence service. They are a processor and must comply with processor obligations under Part 4 for that processing.

What about other key definitions?

You should refer to our general guidance for more information on [what is personal data](#), and what constitutes processing, as these definitions also apply to Part 4. Most definitions used in Part 4 are the same as those used in the rest of the DPA. Section 84 sets out some specific definitions for “consent”;

“employee”; “personal data breach”; “recipient”; and “restriction of processing”. However, these are very similar to the UK GDPR, and the [Guide to the UK GDPR](#) provides useful guidance on their meaning.

What is sensitive processing?

Sensitive processing is defined in section 86(7) of the DPA as:



- (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- (b) the processing of genetic data for the purpose of uniquely identifying an individual;
- (c) the processing of biometric data, for the purpose of uniquely identifying an individual;
- (d) the processing of data concerning health;
- (e) the processing of data concerning an individual’s sex life or sexual orientation;
- (f) the processing of personal data as to –
 - (i) the commission or alleged commission of an offence by an individual, or
 - (ii) 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.



“Genetic data” is personal data relating to the inherited or acquired genetic characteristics of a person. It gives unique information about the physiology or the health of that person and results, in particular, from an analysis of a biological sample from the individual in question.

“Biometric data” is personal data that is obtained through specific technical processing relating to physical, physiological or behavioural characteristics of a person. This processing enables you to identify a particular person, eg fingerprint data and facial recognition.

“Data concerning health” is personal data relating to the physical or mental health of an individual. This includes the provision of health care services, which reveals information about their health status. It can be about an individual’s past, current or future health status. It not only covers specific details of medical conditions, tests or treatment, but includes any related data which reveals anything about the state of someone’s health.

There are close similarities between the types of personal data listed in the Part 4 sensitive processing provisions, and the definitions of special category and criminal offence data under the UK GDPR. The ICO has produced guidance on these provisions under the UK GDPR which contains useful explanations of the definitions of what constitutes [Special category](#) and [Criminal offence](#) data.

Further Reading

 [Key provisions in the DPA 2018 - “Sensitive processing” is defined in section 86\(7\). “Genetic data”, “Biometric data” and “data concerning health” are defined in section 205.](#) 

External link

Who is not covered by Part 4?

You are not subject to Part 4 and will need to comply with a different data protection regime if you are not:

- one of the intelligence services; or
- a processor processing for one of the intelligence services.

If you are a competent authority processing for national security purposes related to your law enforcement purposes, read our [Guide to Law Enforcement Processing](#).

If you are not a competent authority or are not processing for law enforcement purposes, but you are processing for national security purposes, you should read our [Guide to the UK GDPR](#). The usual UK GDPR rules apply, although the DPA provides an exemption where required for the purposes of safeguarding national security, or for defence purposes.

Further reading – ICO guidance

[Which data protection regime?](#)

[About the DPA 2018](#)

[The Guide to Law Enforcement processing](#)

[The Guide to the UK GDPR](#)

[UK GDPR national security exemption guidance](#)

Principles

At a glance

- Part 4 contains six data protection principles:
 - Principle 1 – Lawful, fair and transparent processing
 - Principle 2 – Purpose limitation
 - Principle 3 - Adequate, relevant and not excessive
 - Principle 4 – Accuracy
 - Principle 5 – Storage limitation
 - Principle 6 – Security
- For the processing to be lawful, you must have a Schedule 9 condition for processing.
- If you are carrying out sensitive processing, you also need a Schedule 10 condition for processing.
- You must be able to demonstrate overall compliance with all of the Part 4 principles, except where you can legitimately apply an exemption.

In brief

- [What are the Part 4 data protection principles?](#)
- [What is the first principle?](#)
- [What is the second principle?](#)
- [What is the third principle?](#)
- [What is the fourth principle?](#)
- [What is the fifth principle?](#)
- [What is the sixth principle?](#)

What are the Part 4 data protection principles?

There are six data protection principles in Part 4:

The first data protection principle is that processing must be lawful, and fair and transparent.

The second data protection principle is that processing must be for a specified, explicit and legitimate purpose; and must not be processed in a manner incompatible with the purpose for which it is collected.

The third data protection principle is that personal data must be adequate, relevant and

not excessive in relation to the purpose for which it is processed.

The fourth data protection principle is that personal data must be accurate and, where necessary, kept up to date.

The fifth data protection principle is that personal data must be kept no longer than is necessary for the purpose for which it is processed.

The sixth data protection principle is that personal data must be processed taking appropriate security measures for the risks that arise from the processing.

What is the first principle?



The first data protection principle is that the processing of personal data must be —

- (a) lawful, and
- (b) fair and transparent.

The three elements of lawfulness, fairness and transparency overlap, but you must make sure you satisfy all three. It is not enough to show your processing is lawful if it is fundamentally unfair or lacks transparency.

Fair and transparent processing means that you should, wherever possible, be clear, open and honest about what personal data you process, and what you process it for. We recognise that in many operational matters, given the nature of some intelligence services processing, it may not be possible to be transparent about some of your specific processing activities. You should only handle personal data in ways that people would reasonably expect, and not use it in ways that have unjustified adverse effects on them.

Adverse effects may be fair, if necessary and proportionate. For example, if the use of the data is in the wider public interest. However, you should be able to explain and justify any adverse effects on a case-by-case basis, rather than taking a blanket approach.

How you obtain the data will also have a bearing on fairness. You can only use covert powers where necessary and proportionate. Wherever possible you should avoid misleading the person who is providing the data, as this is more likely to be unfair – unless it is justified in the specific circumstances. The data is deemed to be obtained fairly if you receive it from a person who is:

- authorised by enactment to supply it; or
- obliged to do so by either an enactment or by an international obligation of the UK.

“Lawful processing” means the processing firstly complies with the law, which means any relevant UK law, in particular the legislation governing the activities of the intelligence services. Where relevant, this may

also include ensuring that personal data is obtained in accordance with applicable investigatory powers legislation, and that data is not obtained without a warrant or other authorisation where such a warrant or authorisation is required. It also includes any considerations of necessity and proportionality set out in the European Convention on Human Rights, which the Human Rights Act 1998 incorporates into UK law. Compliance with investigatory powers legislation is overseen by the Investigatory Powers Commissioner.

For the processing to be lawful you must also ensure that you have a Schedule 9 condition for the processing. These conditions are:

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

If you are carrying out [sensitive processing](#) you also need to have a Schedule 10 condition for processing. These conditions are:

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

There is no exemption from the lawfulness element of the first principle, even if you apply the [national security exemption](#). Your processing must always be lawful.

What is the second principle?



The second data protection principle is that –

(a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

The collection of personal data on any occasion must be for specified, explicit and legitimate purposes. In many cases, the intelligence services collect data using powers which are authorised under a warrant or other legal authorisation. For example, under various provisions in the Investigatory Powers Act 2016 (IPA 2016) or the Regulation of Investigatory Powers Act 2000 (RIPA 2000). There are safeguards provided around the issuing of warrants and other authorisations. For instance, what is often referred to as the “double-lock” mechanism, whereby the use of the most intrusive investigatory powers under the IPA 2016 is subject to a two-stage approval process. Rigorous adherence to these safeguards will help to ensure that the purpose for the processing is legitimate.

In cases where the data is collected without a warrant (because a warrant is not required), having first satisfied yourself that the collection is lawful, you need to ensure that you have a specified, explicit and legitimate purpose for the collection of the data, and that you record that purpose.

If you want to use personal data for a different purpose from the one you originally collected it for, you need to ensure your new purpose is compatible with your original purpose (or as the DPA says, “not incompatible”). As a general rule, it is likely to be incompatible with your original purpose, if the new purpose:

- is very different from the original purpose;
- would be unexpected; or
- would have an unjustified impact on the individual.

However, the DPA is clear that you can use the data for any purpose if you are authorised by law to do so, and the processing is necessary and proportionate. Part 4 controllers are in general permitted to process data in so far as it is necessary for their statutory functions, having regard, respectively, to the provisions of the Security Service Act 1989 and the Intelligence Services Act 1994. You must therefore consider necessity and proportionality. The processing will not comply with the second principle if the new purpose is authorised by law, but in the specific context is not necessary or proportionate.

If your new purpose is archiving in the public interest, scientific or historical research, or statistics, this is a compatible purpose – as long as you have put in place appropriate safeguards to protect the rights and freedoms of individuals. You can do this by ensuring that any data processed for these purposes cannot be used to make decisions about individuals, for example by anonymising the data.

What is the third principle?



The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

This principle is often referred to as the data limitation principle. It aims to ensure the data you are processing is of sufficient relevance for your processing. It is important to identify the personal data you need to fulfil your lawful purpose and ensure you are not processing more than you need.

Prior to obtaining the intelligence data, it can be difficult to assess what is relevant, and hence what might

be excessive. Similarly, insufficient intelligence may not be adequate for your purpose if you make decisions about individuals based on too little information to make a properly informed decision.

Compliance with the third principle in this context requires you to consider the intelligence data you collect in order to identify and discard any which is irrelevant or excessive for the purposes for which you collected it. It is inherent to the gathering of intelligence that it is not always possible to immediately assess which information is relevant and of value to your purpose. We recognise that in these circumstances it may be appropriate to retain data for which you have no immediate use. However it is important that you do not collect and retain data indiscriminately. You should be able to justify the retention of any data you hold.

You should also keep in mind the individual's [right to erasure](#) of data.

What is the fourth principle?



The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

The DPA says that inaccurate means “incorrect or misleading as to any matter of fact”.

You must always be clear about what you intend the record of the personal data to show and take reasonable steps to ensure the accuracy of any personal data.

You should ensure that the source and status of personal data is clear in your records. This will help provide context to the information, and assist in your efforts to ensure its accuracy.

Assessment of intelligence is outside the scope of this guidance and is a matter of operational expertise. However, you should assess the accuracy of any data which you rely on when making decisions or taking action, correcting inaccuracies when appropriate and possible to do so. Individuals have a right to rectification or erasure of their personal data and you should carefully consider any challenges you receive from individuals about the accuracy of data you hold about them.

What you use personal data for may affect whether it is accurate or not. You should take this into account when considering the accuracy of the data, alongside other relevant factors. For example, just because personal data has changed doesn't mean that a historical record is inaccurate – but you must be clear that it is a historical record, why you need to retain it, and that doing so is not in itself “excessive”.

You should also consider whether you need to periodically update the information, and also set out how long you expect to continue to hold the information, reviewing this periodically as necessary. This is also relevant to the next principle.

What is the fifth principle?



The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

This is about retention, which must be for no longer than is necessary for the purpose for which the personal data is processed. Although a periodic review is not required, you must be able to demonstrate compliance with the other principles. As a controller you are required, under your [accountability obligations](#), to implement appropriate measures to ensure compliance, and be able to demonstrate these to the ICO. This includes considering the impact on individuals, and implementing measures to ensure that you minimise any risks to their rights and freedoms. Therefore, you are likely to require policies to ensure compliance. A data retention policy is one that would be useful in demonstrating your compliance with the storage limitation principle. There is no maximum retention period set out in the legislation, but you still need to be able to rely on some objective justification for any retention period you set.

What is the sixth principle?



The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

This is about the security of your processing. It means you must have appropriate security in place to take account of the risks of processing personal data. For example, to prevent the personal data you process from being accidentally or deliberately compromised.

This concerns the broad concept of information security, and applies to the processing you do and the environment in which you do it. In particular, you need to:

- design and implement your measures to fit the context of the data you hold and the harm that may result from any incident;
- be clear about who in your organisation is responsible for information security;
- put in place physical and technical security measures to support robust policies and procedures, alongside well-trained staff; and
- make sure you can detect and respond to a breach in a timely manner.

It is your responsibility to determine what these “appropriate security measures” are in the context of your processing and the risks it poses. You should take into account the sensitivity of the data and the consequences for the individual, or for the purpose for processing, of any loss, misuse or damage to the data. You should also consider the current state of the art security methods and techniques.

See [What are our security obligations?](#) for more detail on this.

Further Reading

[Key provisions in the DPA 2018 - see DPA 2018 Part 4, Chapter 2, sections 85 to 91; Schedule 9; and](#)

[Schedule 10.](#)

External link

Individual rights

At a glance

- Part 4 provides individuals with a number of rights, including:
 - the right to information;
 - the right of access;
 - the right to object;
 - the right to rectification;
 - the right to erasure; and
 - rights in relation to automated decision-making.
- Under Part 4 you can charge a fee for dealing with a subject access request. The level of this fee may be set by the Secretary of State in regulations but, in the absence of any such regulations at this time, the maximum fee is set at £10.
- You should communicate any information that you are required to provide by Part 4 in clear and plain language.
- Individuals can exercise their rights by making a complaint to the ICO or taking matters to court.

Checklists

- We make information available about how we process personal data. This information is clear and easy to understand.
- We know how to recognise a SAR and we understand when the right of access applies.
- We understand what steps we need to take to verify the identity of the requestor, if necessary.
- We have processes in place to allow individuals to exercise their rights, and to deal with these promptly and within the correct time limit.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

In brief

- [What rights do individuals have?](#)
- [What is the right to information?](#)
- [What is the right of access?](#)
- [What is the right to relating to decision-making?](#)

- What are the rights around automated decision-making?
- What is the right to object?
- What is the right to rectification?
- What is the right to erasure?

What rights do individuals have?

Individuals have a number of information rights in Part 4:

- The right to information about the processing.
- The right of access.
- The right to information about decision-making.
- Rights around automated decision-making.
- The right to object.
- The right to rectification.
- The right to erasure.

These rights may be restricted by the application of the national security exemption, or other exemptions listed in Schedule 11 of the DPA, where required.

What is the right to information about the processing?

This is a right for individuals to be proactively informed about the processing that is happening. It is distinct from the right of access to an individual's own personal data, and is closely connected to the transparency aspect of the first principle.

The right to information does not distinguish between whether data is collected from the individual directly, or indirectly from another source.

The information you need to provide is:

- your identity and contact details as controller;
- the legal basis on which you are processing personal data;
- the purposes for which you are processing personal data;
- the categories of personal data relating to the individual that you are processing;
- the recipients or the categories of recipients of the personal data (if applicable);
- the right to lodge a complaint with, and contact details of, the ICO;
- how to exercise their data protection rights; and
- any other information that is needed to ensure that the personal data is processed fairly and transparently.

The nature of covert intelligence and analysis necessarily imposes limits on what you can say, but you should aim to be as transparent as possible. When providing "any other information" you should include any other relevant details which help individuals and the public at large understand the nature and context of the processing, and inform their reasonable expectations. You should consider whether there is anything

else you can reasonably provide which would help people understand what's going on. This will ensure your processing is not unexpected and the privacy information is not misleading. This will help you demonstrate your compliance with the fairness element of the first principle.

How you provide this information is up to you, but you should be able to justify your decisions – in particular if you decide to provide this information by a generally available notice.

Quite a lot of this information is likely to be fairly generic and won't vary from person to person. For example, who you are and what you do, your lawful basis for processing, and what categories of personal data you process. In this case a public notice may be appropriate, although the most appropriate way to provide it will depend on the context (eg on your website, intranet or in a notice to a contractor).

What is important is that the relevant information is made readily available to the relevant target audience. For example, your intranet is not an appropriate method to communicate information to the general public, but is appropriate for telling your staff how you process employee data. When making a decision about what method to use, consider the ways you can effectively provide the information and the audiences it will reach, making sure you do not miss categories of people you need to provide the information to.

You are not required to provide this information if:

- the individual already has the information; or
- you obtained the data from a third party and it is impossible, or would involve disproportionate effort, to provide it to the individual.

To rely on the "disproportionate effort" provision, you must assess (and document) whether there is a proportionate balance between the effort involved for you to provide individuals with privacy information and the effect that your use of their personal data will have on them.

It is highly unlikely that these provisions will apply, if you are in a situation where it would be appropriate to publish general information about your processing by a generally available notice. For example, a privacy notice on your website. You should therefore provide privacy information in this way.

You are not required to provide information to the individual if you collect their data indirectly and this is authorised by an enactment. For example, under the IPA 2016 (which provides various powers for the intelligence services to obtain information).

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and to check you are doing it lawfully.

Under this right, individuals can obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data in intelligible form. This includes providing an explanation of any technical terms or jargon which might otherwise obscure its meaning to the reader; and
- other supplementary information (this largely corresponds to the information that you should provide in a privacy notice).

You should comply with a subject access request (SAR) by providing the individual with a copy of their data in writing, unless:

- this is not possible;
- would involve disproportionate effort; or
- the individual agrees to receive it in another form.

When considering whether providing a copy would involve disproportionate effort, you should consider the effort required in doing so against the value to the individual of receiving that copy. If you decide that it would be disproportionate, you should record your reasons, and be able to explain them to the individual and the ICO.

You can charge a fee for a SAR under Part 4. The level of this fee may be set by the Secretary of State in regulations but, in the absence of any such regulations at this time, the maximum fee is set at £10.

You need to be satisfied that you know the identity of the requester. If you are unsure, you can ask for information to verify an individual's identity. You can ask for enough information to judge whether the requester is the person that the data is about. The key point is that you must be reasonable and proportionate about what you ask for. You should not request more information if the requester's identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

The timescale for responding to a SAR does not begin until you have received the requested information. However, you should request ID documents promptly.

There may also be times when you need additional information from the individual in order to identify and locate the data that they are requesting. This may particularly be the case if the request is phrased in very broad and general terms. You should not seek clarification on a blanket basis, and only if you genuinely require it in order to locate the requested information and respond to a SAR. Again, the timescale for responding to a SAR doesn't begin until you have received the additional information. You should request this additional information promptly.

If you have previously complied with a request, you don't have to respond to a repeat request for the same information, unless a reasonable interval has elapsed. When deciding whether a reasonable interval has elapsed you should consider:

- the nature of the data (including whether it is particularly sensitive);
- the purpose you are processing the data for; and
- how often you alter the data.

If it is unlikely that the data has changed between requests, you may decide you do not need to respond to the same request twice (although you should still acknowledge it). However, if you have deleted data since the last request, you should inform the individual of this.

In some cases the requested data may also contain information relating to another individual (including any references identifying an individual as the source of the data). You should then consider whether it is possible to comply with the request without disclosing information that identifies the other individual. For example, by omitting their name or other identifying information. If this is not possible, you do not have to disclose the information except where:

- the other individual consents to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without their consent.

You should keep a record of what you decide and why.

You need to provide the information to the individual 'promptly' and, in any event, within one calendar month of receiving it (ie within one calendar month of the day you received the request). If you have requested a fee, additional identification, or further information to locate the data requested, the one month time period begins on the day you receive it.

If you are unable to comply with a request, you should inform the individual about:

- the reasons why (where possible);
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts.

If you are relying on an exemption to refuse to comply with a SAR, where possible you should explain the reasons why you consider this exemption applies. However, this will depend on the specific circumstances of the request. In some situations, your response may be more general and may not include details of which exemptions you have relied on at all. For example, where telling an individual that you have applied a particular exemption would prejudice the purpose of that exemption.

What is the right relating to decision-making?

Where you are processing data and applying the results to an individual, section 98 says that they have the right to know the reasoning underlying that processing. This applies whether the processing and results (or decision-making) are automated or not. There isn't a requirement to proactively give this information to the individual, but if it is requested you must provide it promptly and without undue delay.

What are the rights around automated decision-making?

You should not make any decision solely by automated means that significantly affects an individual, unless:

- the decision is required or authorised by law;
- the individual has given consent to the decision being made this way; or
- it is needed for entering into or performing a contract with the individual.

A significant effect is not defined, but includes a decision which has a legal effect on an individual (whether adverse, or not). However, this is not the only factor, and you need to take into account the significance of any decision of this nature on an individual – taking into account the specific circumstances.

This right only applies to automated decision-making. This is where decisions are made about individuals automatically, and without human input or intervention. This is distinct from "automated processing" (eg the collection, storage, or other processing by IT systems or other automated means) – although automated processing will be involved in automated decision-making.

If the automated decision is required or authorised by law, you must notify individuals that such a decision

has been made and that they have a right to request human intervention in that decision-making. They can request the decision is reconsidered, or request that a new decision is taken which isn't based solely on automated processing.

You must consider any request, including any relevant additional information the individual provides, and inform them in writing of the outcome of that consideration.

This right to be notified, and to have intervention, doesn't apply if the automated decision-making was done:

- with the consent of the individual; or
- for the purposes associated with entering into or performing a contract with them.

What is the right to object?

Individuals have the right to object to the processing of their personal data (either in general or in relation to a specific purpose), on the grounds that they believe that the processing is an unwarranted interference with their rights or interests. The individual must inform you of their specific reasons why they believe the processing constitutes an interference, and why it is unwarranted in the circumstances. If you receive an objection you should consider it. You may continue with the processing while you are considering the objection.

If you decide to agree to the objection, you must stop the processing. If, having carefully considered the necessity and proportionality of the processing, you decide that in the circumstances the processing is not an unwarranted interference, you can continue processing.

Whether or not you agree with their objection, you must inform the individual of your decision within 21 days, and give your reasons. If you need to verify the ID of the requester, or need further information to locate the data in question, this period doesn't start until you have received the information you reasonably require. If you do not comply with an objection from an individual, they can challenge this through the courts.

What is the right to rectification?

Individuals have the right to request the rectification of their personal data if they believe it is inaccurate.

As a matter of good practice, you should put in place processes that allow individuals to inform you of any concerns they have about the accuracy of data you are processing about them. You should also establish a mechanism for assessing these concerns and making corrections or adjustments to data that you hold, if you think these are necessary. You should also make a record of the reasons behind your decisions, as this will assist you if the individual takes the matter to court.

Taking these steps will assist you in complying with the data limitation, storage limitation and accuracy principles. It will also help to ensure you effectively implement individuals' rights in line with your general accountability obligations.

An individual can seek to enforce this right through the courts. The court may order you to rectify the data without undue delay.

In certain circumstances the court may order that the processing of the data is restricted, as an alternative to rectification. This may occur if:

- the data in question must be maintained for evidential purposes; or
- an individual contests the accuracy of data, and the court decides that you cannot determine its accuracy.

“Restriction of processing” is defined as marking stored data with the aim of limiting its processing for the future.

An individual may also make a complaint to the ICO if you fail or refuse to rectify inaccurate data.

What is the right to erasure?

Individuals have the right to request the erasure of their personal data if they believe the processing of the data contravenes any of the data protection principles.

As a matter of good practice you should put in place processes that allow individuals to request the erasure of their personal data, and for you to consider these requests. You should make a record of your decision-making.

An individual can seek to enforce this right through the courts, and the court may order you to erase the data without undue delay.

Alternatively the court may order that you restrict the processing of the data, rather than erase it. This may occur if:

- the data in question must be maintained for evidential purposes; or
- the accuracy of the data has been challenged, and the court decides that you cannot determine its accuracy.

An individual may also make a complaint to the ICO about a failure or refusal to rectify inaccurate data.

Further Reading

 [Key provisions in the DPA 2018 - see DPA 2018 Part 4, Chapter 2, sections 92 to 100.](#) 

External link

Obligations

At a glance

- It is your responsibility to ensure compliance with the provisions of Part 4, and to be able to demonstrate this to the ICO.
- You must consider the impact of processing on individuals, and implement measures to ensure you comply with the principles and minimise the risks to the rights and freedoms of individuals.
- You must implement appropriate security measures.
- You must report serious personal data breaches to the ICO. A breach is serious if it seriously interferes with individuals' rights and freedoms.
- You may only transfer personal data outside the UK if this is necessary and proportionate for your statutory functions or certain statutory purposes.

In brief

- [What accountability obligations do controllers have?](#)
- [What obligations do processors have?](#)
- [What are our security obligations?](#)
- [What do we have to do if there is a personal data breach?](#)
- [What are the rules on transfers?](#)

What accountability obligations do controllers have?

If you are a controller, you have an obligation to ensure that your processing complies with the requirements of Part 4, and that you are able to demonstrate this to the ICO. The [national security exemption](#) does not apply to this obligation, so you must ensure that your processing remains compliant and that you are able to demonstrate this at all times. Although there is no legal requirement to appoint a Data Protection Officer (DPO) under Part 4, you may decide to appoint a member of staff with a similar role in order to assist you in ensuring and demonstrating compliance to the ICO.

You also have to implement the principles of data protection by design, by introducing measures to consider the impact of your processing on the rights and freedoms of individuals and minimise the risks to them. While there is no specific obligation to conduct a Data Protection Impact Assessment (DPIA) it is one good way to assess and demonstrate your compliance. The ICO has issued [guidance about how you can undertake a DPIA under the UK GDPR](#), which may give you useful points to consider.

Two or more intelligence services can operate as joint controllers when they jointly determine the purposes and means of processing. In these cases, you are obliged to determine who is responsible for:

- the different aspects of the processing; and
- responding to individuals who are exercising their information rights under Part 4.

There may be working relationships between the intelligence services and Part 3 competent authorities (eg

police counterterrorism units) or UK GDPR controllers. However, these cannot be joint controller relationships. This does not prevent other controllers working with the intelligence services. It just means that they will each operate as controllers independently for their own processing, not in a joint controller arrangement.

You may use processors to carry out processing of personal data on your behalf. You may only use a processor that implements sufficiently appropriate measures to ensure their processing complies with Part 4, and provides you with all the necessary information to demonstrate their compliance.

While there is no explicit requirement for a contract between you and a processor, the requirements mean that you need a clear agreement. This should set out not only the extent and limits of the processing, but also the measures they are taking to ensure compliance with Part 4.

What obligations do processors have?

As a processor you must undertake to the controller to:

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

Processors do not have the same obligations or responsibility as controllers. However, if you are a processor, you do have some direct obligations of your own under Part 4:

- You may only process personal data on instructions from the controller, or to comply with a legal obligation that applies to you. Remember that if you process data to comply with your own legal obligations, you are a controller for this element of the processing and need to comply with the UK GDPR or Part 3 of the DPA, as appropriate.
- You must implement appropriate security measures.
- You must inform the controller without undue delay if you become aware of a personal data breach.

The ICO may take action against a processor who fails to comply with these obligations.

As a processor, you may not determine the purposes and means of the processing. If you act outside the controller's instructions, the processing will be in breach of the DPA. You will be treated as the controller, and held responsible for that unlawful processing.

What are our security obligations?

Each controller and processor must implement security measures appropriate to the risks arising from that processing. Although this obligation applies to both, it is the controller's responsibility to:

- satisfy yourself that any processors you engage are able to meet appropriate security standards; and
- set out clearly what security measures processors are required to adhere to.

When considering what's appropriate, you should think about:

- the potential adverse consequences for an individual of any compromise;
- the nature and volume of the data you process;
- the degree of vulnerability in the processing environment;

- any need to restrict access to the data; and
- any requirements concerning long-term storage (eg any security or integrity issues brought about by the need to retain information).

These are not exhaustive examples. However, given that the purposes, in a national security context, are likely to be highly sensitive, and the data therefore is sensitive to loss, misuse or damage, it follows that appropriate security measures need to reflect this. You may need to maintain security at a much more rigorous level than for less sensitive purposes.

The measures you put in place should also take into account the:

- state of the art of available security techniques and methods – taking into account their suitability for the specific processing in question;
- likelihood and severity of the potential risks; and
- need for regular review and updating, where necessary.

Remember that putting in place appropriate security measures isn't just about cyber-security or technical measures, which concern protecting network and information systems from attack. It also includes physical and organisational security measures that are appropriate in the context of your processing. These may include policies and procedures about administrative measures, vetting, access controls, training, codes of practice and disciplinary provisions.

You also need to ensure suitable provisions are set out and followed by any processors you use.

You must evaluate the risks for any form of automated processing (ie any processing done on automated systems, which is generally taken to mean IT systems). This includes both you or any processors working on your behalf. You and your processors have to implement measures designed to:

- prevent unauthorised processing or unauthorised interference with the systems used in connection with the processing;
- establish the precise details of the processing;
- ensure systems function properly and can be restored in the case of interruption; and
- ensure that stored data can't be corrupted in the event of a malfunction of a system.

These measures could include:

- records management and logging processes that enable you to audit access to, and processing of, personal data;
- technical and organisational methods to verify the integrity of the data you hold, and ensure you can restore it;
- establishing specific security clearance levels for staff in terms of physical access as well as network and information systems, in accordance with the principle of least privilege; and
- protections for your network and information systems to prevent unauthorised access.

Further reading – ICO guidance

The ICO has also produced guidance on [Security](#) for controllers operating under the UK GDPR which provides further useful detail.

What do we have to do if there is a personal data breach?

Section 84(4) defines a personal data breach as:



A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A breach of your data security measures may be accidental, or intentional (eg a deliberate or malicious breach of security). A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach:

- whenever any personal data is lost, destroyed, corrupted or improperly disclosed
- if someone accesses the data or passes it on without proper authorisation; or
- if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Section 108 sets out obligations on controllers to notify the ICO of a “serious personal data breach” without undue delay. There isn’t a statutory obligation to report within 72 hours of becoming aware of it, but if notification doesn’t occur within that period, you’ll need to include an explanation for the delay when you do notify.

The requirement to notify a ‘serious’ personal data breach means that you need to notify the ICO of all breaches that are considered serious. This will require you to consider:

- the severity of the impact on the rights and freedoms of the affected individuals;
- the scale of the data breach (ie how many people are affected);
- the extent of any interference with the right to privacy under Article 8 of the European Convention on Human Rights (ECHR);
- whether the breach involves any personal data whose processing constitutes “sensitive processing”; and
- the nature of the rights and freedoms which have been impacted (eg a breach leading to a risk to the right to life under Article 2 ECHR would be particularly serious).

Consequences could be anything which seriously interferes with an individual’s rights and freedoms. It is for you to decide whether a personal data breach meets the threshold to be considered serious.

When you report a serious data breach, you need to include:

- a description of the nature of the breach, including where possible the categories and approximate number of affected individuals, and the categories and approximate number of records concerned;
- a contact point for the ICO to obtain more details (if you have appointed a DPO it is likely this will be their details);

- a description of the likely consequences of the breach; and
- your proposals to deal with or mitigate the effects of the breach (eg you should consider whether to notify the affected individuals of the breach).

You may not be able to provide all this information straight away, and you shouldn't delay reporting a breach until you have collated all this information. Instead, you can provide the information in phases as soon as you have it. [The ICO and the intelligence services have set out, in a Memorandum of Understanding \(MoU\)](#), the process whereby data breaches will be reported, and arrangements for any subsequent investigation or regulatory action the ICO intends to take.

If a personal data breach is also a "relevant error" as defined at section 231(9) of the IPA 2016, you don't have to report it to the ICO. Instead you need to follow the reporting requirements in the IPA 2016 and report the error to the Investigatory Powers Commissioner's Office.

Processors have to notify the controller "without undue delay" if they become aware of a breach. This is not restricted to 'serious' breaches, as defined above. It is the responsibility of the controller to determine whether a breach meets the criteria to be designated as serious (and therefore, reportable to the ICO). Therefore the processor should report all breaches to you, so you can make this assessment. You should include this requirement in any agreement setting out the arrangements between controller and processor.

What are the rules on international transfers?

There are restrictions on the transfer of personal data to a country or territory outside the UK, or to an international organisation. A transfer of personal data is only permissible if the transfer is a necessary and proportionate measure carried out for:

- the purposes of the controller's statutory functions; or
- other purposes in relation to the controller, provided for in section 2(2)(a) of the Security Services Act 1989, or section 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994.

You need to consider whether the transfer is necessary and proportionate for the purposes of your statutory functions. This means those functions set out in the governing legislation about the service's wider role in safeguarding national security or tackling serious crime.

Part 4 provides no further specific safeguards for transferring personal data outside the UK (although the other requirements of Part 4 still apply). However, you are subject to other legislative restrictions under the various enactments which govern the work of the intelligence services, such as (but not restricted to) those referred to in the second bullet point above. These contain measures to ensure that personal data is obtained, shared and handled lawfully and responsibly. You should also consider the extent to which you may require additional security measures to protect transfers. If a transfer under section 109 were to lead to a breach of Part 4 of the DPA, the ICO has powers to investigate and take action.

Exemptions

At a glance

- There is an exemption that you may apply to many of the principles, rights and obligations, and some of the powers of the ICO, where you consider it is reasonably necessary to safeguard national security.
- This is not a blanket exemption. You 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.
- A Minister of the Crown (specifically a member of the Cabinet, the Attorney General or the Advocate General for Scotland) can issue a certificate which covers the processing. If they do so, this is conclusive proof that the exemption applies in the circumstances described in the certificate. We publish details of relevant certificates.
- You must always still have a lawful basis for your processing. You must also still comply with your general accountability and security obligations.
- There are also a number of other specific exemptions available.

Checklist for using the exemption

- We have a lawful basis for our processing.
- We have complied with our documentation and other accountability obligations.
- We can point to a clear link between compliance with a specific provision and a potential adverse effect or difficulty for our operational work to protect national security.
- We do not apply the exemption in a blanket manner, and have considered the circumstances of the case.
- We have considered whether a national security certificate is applicable in the circumstances.

In brief

- [What is the national security exemption?](#)
- [How does the national security exemption work?](#)
- [What are national security certificates?](#)
- [Are there any other exemptions?](#)
- [How do the Schedule 11 exemptions work?](#)
- [What harm-based exemptions are available?](#)
- [What class-based and gateway exemptions are available?](#)

What is the national security exemption?

Section 110 sets out an exemption that may be applied to many of the data protection provisions:



“...if exemption from the provision is required for the purpose of safeguarding national security.”

If the exemption applies, it can exempt you from:

- any of the principles (except the lawfulness requirement);
- any of the rights of individuals;
- personal data breach reporting; and
- some of the powers of the Commissioner.

However, you must always ensure your processing is lawful, and that you have a lawful condition for your processing under Schedule 9.

If you are carrying out sensitive processing, you must also ensure you have a relevant condition for sensitive processing under Schedule 10.

You must also still comply with your general accountability and security obligations.

We may investigate your compliance, and will generally consider whether you have properly claimed an exemption. The [MoU between the Commissioner and the Intelligence Services](#) provides more detail of how we investigate complaints.

How does the national security exemption work?

Given the importance of national security, you can apply this exemption to a greater number of provisions than many other exemptions.

National security is not specifically defined, and can be interpreted in a flexible way to adapt to changing threats. Thirty years ago, it would have been difficult or even impossible to predict the threats that developments in computer and communications technology could give rise to, or how such developments could be exploited by terrorists or hostile states. It is 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 terrorists or hostile states;
- protection of potential targets even in the absence of specific threats; and
- international co-operation with other countries.

The exemption applies if it is “required” to safeguard national security. In this context, “required” means that the use of the exemption is “reasonably necessary”. This is linked to human rights standards and your obligations under the Human Rights Act 1998 and the European Convention on Human Rights (ECHR). This means that any interference with privacy rights should be necessary and proportionate in a democratic

society to meet a pressing social need.

The exemption can be applied flexibly and to a large number of the data protection provisions. However, it is not a blanket exemption. You must consider the actual consequences to national security, or to your work in safeguarding national security, if you had to comply with the particular DPA rule. In other words, you should apply the exemption only when it is necessary and on a case-by-case basis. If you could reasonably comply with any of the usual rules without affecting your work, you must do so.

You don't need to show that compliance would lead to a direct or immediate harm or threat. It is enough to show that there is a real possibility of an adverse effect on protecting national security in a broader sense. For example, in freedom of information cases, courts have recognised that terrorists can be highly motivated. There may therefore be grounds for withholding seemingly harmless information on the basis that it may assist terrorists when pieced together with other information.

If you use the exemption, you are still accountable to the ICO for your compliance with the DPA and you should be able to make a reasoned and convincing argument about the risks of compliance with the specific provision. You may base these on hypothetical scenarios, as long as they are realistic and credible.

For example, you may need to use the exemption to maintain a consistent line so that individuals cannot draw inferences which might harm national security in other cases. For example, to give a non-committal "neither confirm nor deny" (NCND) response to subject access requests.

Example

An intelligence service receives a SAR from a member of the public, who suspects that they may be under surveillance. The service doesn't hold any relevant personal data about the individual, because they are not a person of interest. But they do not wish to let the person know that no relevant information is held because, if they actually are involved in matters which would be of concern, this may tip them off that their activities have not aroused suspicion. Moreover, if an individual did apply who was under surveillance, the service would want to neither confirm nor deny this. This means that they must adopt a consistent approach, to avoid the applicant knowing whether they were under surveillance or not.

There is no obvious prejudice to national security if no personal data is held, because there is no evidence held that suggests the person is engaged in any activity which would present a risk to national security. But the exemption could still be available if the response to the SAR might expose weaknesses in the intelligence about the person, or in order to avoid indicating whether an individual was or was not under surveillance.

The intelligence service could issue a response to the SAR which didn't alert the individual whether personal data was or was not held (a NCND response), and could apply the exemption at section 110 to the extent necessary to avoid any relevant, specific requirements of responding to subject access requests.

You can apply a NCND response as a general policy. However, you cannot apply it in a blanket manner, because there may be circumstances in which it is not required for the purposes of safeguarding national

security. As a result, you should still consider whether there are any special circumstances which mean you don't need to rely on the general NCND policy in a particular case.

In many cases we may investigate compliance and consider whether you have properly claimed an exemption, or otherwise complied with Part 4. The ICO retains all our powers and regulatory functions where the use of these would not adversely affect the protection of national security. However, sometimes it may not be possible for us to exercise these powers, if our investigation might adversely affect your work in safeguarding national security. We have agreed a [Memorandum of Understanding with the Government](#), which sets out our understanding of how this may work in some anticipated circumstances, such as a data breach or a complaint.

What are national security certificates?

A Minister of the Crown (specifically a member of Cabinet, the Attorney General or the Advocate General for Scotland) can sign a certificate which is conclusive evidence that the exemption is required for the purpose for safeguarding national security. These certificates can be issued in advance or retrospectively, so it isn't always necessary for a certificate to be in place before claiming the exemption. The personal data to which the certificate applies may be identified in general terms.

The national security exemption can still apply even if a national security certificate has not been issued. However, the existence of a certificate is conclusive evidence that the exemption applies to the data described in the certificate. If a relevant certificate is in place, you may rely on it to demonstrate that the exemption applies.

The ICO [publishes the existence of the certificates](#), and basic details including the name of the Minister who signed it and the date of signing, together with the text of the certificate where possible. However, there may be some cases where elements are redacted or the text is withheld, if the Minister decides that publishing would be:

- against the interests of national security;
- not in the public interest; or
- would jeopardise the safety of any person.

In all other circumstances, we will publish the full text of the certificate.

A person directly affected by the issuing of a certificate may appeal to the Upper Tribunal. The Tribunal can quash the certificate if it considers that the Minister did not have reasonable grounds for issuing it.

In some circumstances, an individual can also appeal to the Upper Tribunal to challenge whether a certificate applies to their personal data. This right of appeal only applies where they are already party to court proceedings under the DPA (eg to enforce their right of access or objection), and the intelligence service relies on a certificate in those proceedings which applies to a general category of data.

The fact an applicable national security certificate exists does not mean you should rely on it in all circumstances. Even though a certificate has been issued, there may be occasions where there wouldn't be any adverse effect on your work in safeguarding national security if you complied with a provision in Part 4. In such cases, you cannot rely on the exemption, even if a certificate has been issued about the personal data in question.

Are there any other exemptions?

Schedule 11 contains further exemptions. These may be thought of as 'specific' exemptions, in that they relate to a specific set of circumstances and permit exemption from certain provisions of Part 4.

Where necessary, they provide exemptions from:

- the data protection principles (as set out in Part 4), except that the processing must always be lawful and meet a relevant condition for processing as set out in Schedule 9 and 10;
- the rights of individuals; and
- duties relating to reporting breaches to the ICO.

They do not provide an exemption from the powers of the ICO to investigate complaints about the application of the Schedule 11 exemptions, or the general accountability and security obligations of controllers and processors.

You should remember that although exemptions are available for use where required, in most circumstances their use is not mandatory. You can choose not to apply an exemption which would otherwise be available to you. However, there may be some circumstances where you are compelled to apply an exemption. For example, where Parliamentary Privilege applies, or where information is required to be made public by law.

How do the Schedule 11 exemptions work?

The exemptions are mostly intended to:

- avoid some form of harm or prejudice (harm exemptions); or
- permit something to be done which would otherwise not be permissible (gateway exemptions).

There are also a number of class-based exemptions that you can apply if the information conforms to the description in the exemption. They are similar in purpose and effect to several of the exemptions in the UK GDPR found at Schedule 2 of the DPA. For more detailed consideration of how you may apply them, you may find it helpful to refer to our [guidance on the UK GDPR exemptions](#) as many of the principles and considerations will be similar.

The applicable purposes of the exemptions are summarised below. For the specific wording of any exemption refer to the relevant paragraph of Schedule 11.

What harm-based exemptions are available?

The harm exemptions are for the avoidance of prejudice or harm to:

- prevention and detection of crime, or the apprehension and prosecution of offenders (paragraph 2);
- judicial proceedings (paragraph 5);
- the combat effectiveness of the armed forces of the Crown (paragraph 7);
- the economic well-being of the UK (paragraph 8); and
- negotiations with the data subject (paragraph 10).

In all cases, you can only apply the exemption to the extent that you need to in order to avoid the prejudice or harm listed in the exemption.

The test is in most cases whether the DPA provision, if applied, “would be likely to prejudice” the activity specified in the exemption. This requires a two-part test.

Firstly, the prejudice or harm envisaged has to be more than trivial, so that the risk outweighs the importance of adhering to the DPA provision in question.

Secondly, the likelihood of the harm occurring has to be a real possibility, and not just remote or fanciful. In short, you need to be able to show that there is a realistic likelihood of some form of harm occurring, and that avoidance of this harm is sufficiently important that it requires you to exempt the processing from the DPA provision you are applying the exemption to.

In addition, there is also an exemption for scientific or historical research, or statistical or archiving purposes (paragraphs 13 and 14). This exemption is only available if:

- the personal data is processed subject to appropriate safeguards for the rights and freedoms of the data subject; and
- none of the statistics made available identify a data subject.

This exemption is only available to the extent that the DPA provision would prevent or seriously impair these purposes. This is a different, and somewhat higher hurdle than ‘prejudice’ and requires you to show that the DPA provision in question would actually prevent you from carrying out the activity, or otherwise make it very difficult for you to carry it out.

Keep in mind also that you cannot use these exemptions in a blanket fashion, but must apply them selectively and in as limited a manner as possible, sufficient to avoid the prejudice.

Example

An intelligence service is negotiating a settlement with a former employee who is pursuing an employment claim. The individual has made a subject access request, requesting information about the service’s willingness to compromise. In such circumstances the intelligence service may refuse to provide the former employee with information about their negotiating position, where this would prejudice the negotiations themselves (Schedule 11, paragraph 10). If there is no appreciable risk of prejudice, then the exemption would not be available (for example, because the negotiations are concluded).

If you apply an exemption, it is important to clearly record the reasons for its application, so that if necessary you can explain these to the ICO.

What class-based and gateway exemptions are available?

There are several exemptions you can use for data which matches one of the descriptions in the exemption. If this is the case, you don’t need to show that there would be prejudice in order to apply the exemption:

- Parliamentary privilege (paragraph 4).
- Information about the conferring of Crown honours and dignities (paragraph 6).
- Legal professional privilege (paragraph 9). This exemption recognises the importance of preserving the principles of legal privilege. Both advice and litigation privilege are covered by this exemption.
- Confidential employment, training or education references (paragraph 11). This exemption permits the intelligence service to exempt a confidential reference it has given.
- Exam scripts and marks (paragraph 12). This prevents obtaining details of a candidate's examination answers, or the marks received, before the results of the examination are announced.

These exemptions recognise the inherent confidentiality in certain processes and allow you to protect and preserve that confidentiality where necessary. Again, you should apply the exemptions as restrictively as possible, consistent with the purpose of the exemption. In some cases, for example Parliamentary Privilege, you may have a legal obligation to uphold the privilege and the exemption allows you to meet these obligations.

There is one gateway exemption which applies if:

- personal data is required to be made public by law; or
- disclosure is necessary for the purpose of legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights (paragraph 3).

You can use this exemption to permit disclosure of information which would otherwise not be permitted under Part 4. For example, if the disclosure would otherwise breach an individual's rights.

This exemption can also apply to prospective legal proceedings. Therefore, it is available even if the proceedings have not yet been commenced and are just at the fact finding or obtaining legal advice stage.

Further Reading

 [Key provisions in the DPA 2018 - see DPA 2018 Part 4, Chapter 2, sections 110 to 112; and Schedule 11](#)

External link

If you are not an intelligence service, then this guidance does not apply to you. If you are a competent authority processing for law enforcement purposes, Part 3 of the DPA contains provisions that allow you to restrict the rights of individuals or limit your obligations where this is required to protect national security. See our [guidance on the Part 3 national security provisions](#) for more details.

For all other controllers and purposes, you are processing under the UK GDPR, and may be able to use the national security exemption at Section 26 of the DPA. See our [guidance on the application of the national security exemption](#).