Data protection

Guide to Law Enforcement Processing

ico.
Information Commissioner's Office

About the Guide to Law Enforcement Processing

The Guide to Law Enforcement Processing is part of our Guide to Data Protection. It is for those who have day-to-day responsibility for data protection in organisations with law enforcement functions.

It explains the data protection regime that applies to those authorities when processing personal data for law enforcement purposes. It covers part 3 of the Data Protection Act 2018 (DPA 2018), which is separate from the UK GDPR regime.

It explains each of the data protection principles, rights and obligations. 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 and relevant European guidance published by the European Data Protection Board (EDPB). EDPB guidelines are no longer directly binding to the UK regime, but are included as a useful reference resource.

This section only covers processing for law enforcement purposes. You will need to read our Guide to the UK GDPR when processing for non-law enforcement purposes.

Scope and key definitions

At a glance

- Part 3 only applies to competent authorities (or their processors) processing for criminal law enforcement purposes.
- Processing for other general purposes such as HR will fall under the general processing regime in part 2 of the DPA 2018.
- It applies to processing of personal data, which is information about identifiable living individuals.
- Controllers determine 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.

In brief

Who does Part 3 apply to?

Part 3 only applies to competent authorities processing for law enforcement purposes. So, it applies, but is not limited, to:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

The appropriate regime is based on the law that applies to the controller. So if you are a processor carrying out a law enforcement function on behalf of a competent authority, you will also be processing under this law enforcement processing regime.

Any processing carried out by a competent authority which is not for the **primary purpose** of law enforcement will be covered by the general processing regime under the UK GDPR(read with Part 2 of the DPA 2018.

If you are a competent authority it is very likely that you are also processing personal data under the

general processing regime. For example, this may include internal HR processes and procedures, as that processing isn't strictly for law enforcement purposes.

Identifying the correct regime is important as there are many key differences between the general processing regime and Part 3 of the DPA 2018, including differences on individuals' rights, lawful basis for processing and governance.

What is a 'competent authority'?

A competent authority means:

- a person specified in Schedule 7 of the DPA 2018; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

You need to check whether you are listed as a competent authority in Schedule 7 of the DPA 2018.

If you are not listed in Schedule 7, you may still be a competent authority if you have a legal power to process personal data for law enforcement purposes. For example, local authorities who prosecute trading standards offences or the Environment Agency when prosecuting environmental offences.

Further Reading

Relevant provisions in the DPA 2018 - See Section 30 and Schedule 7
External link

Are we processing for law enforcement purposes?

If you are a competent authority, when you are deciding which regime applies, the key thing to consider is your **primary purpose** for the processing. This should help you identify whether the processing falls under the UK GDPR rules, or satisfies the criteria of the law enforcement purposes under Part 3 of the DPA 2018.

The law enforcement purposes are defined under section 31 of the DPA 2018 as:

> 'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

So if you are a competent authority processing for one of those purposes, you should comply with the law enforcement processing regime.

Example

A police officer is called to a disturbance where allegations of assault have been made. The officer attends the scene using their body-worn camera. Witnesses are interviewed and this footage is recorded on the body-worn camera.

The footage is recorded and processed to investigate the crime. So the processing is carried out for the prevention, investigation, detection or prosecution of criminal offences. Part 3 of the DPA 2018 applies.

What if we are processing for other general purposes?

Even if you are a competent authority, in some circumstances, you may also process data for **general purposes,** such as for your own HR purposes. If processing is not for the law enforcement purposes, it will fall into the general processing regime in the UK GDPR read with and Part 2 of the DPA 2018 you should refer to our Guide to the UK GDPR.

Example

A police force want to obtain information from the public about their perception of the force in general. The results will help influence how the force engage with the public. They therefore conduct a survey to capture people's views.

Personal information is collected about individuals, but the primary purpose of the processing is to gain an insight into their opinions of the force. So the processing is not to prevent and detect crime.

In this case, the relevant regime is the general processing regime, and you should read our Guide to the GDPR.

What happens if our purpose changes?

You may begin processing information under one regime, but as circumstances progress and the purpose changes, the processing of the data will come under another regime or take place under both simultaneously.

You may initially be processing data for general administrative purposes, but as the situation changes you may identify elements of criminality. The processing would then come under Part 3 of the DPA 2018. It may be easier to identify a change in regime if the data is passed to a specialist team or department to continue the processing for a specific purpose. For example, a dedicated fraud unit may obtain information originally collected under the general processing regime for the purposes of an investigation under Part 3 of the DPA 2018.

Likewise, in certain circumstances the processing of information by a competent authority may begin under the law enforcement processing regime in Part 3 of the DPA 2018, and as circumstances change, it may switch to the general processing regime. Some information may end up being processed for different purposes and under both regimes.

Any information that is being processed for law enforcement purposes must adhere to the governance requirements of Part 3 of the DPA 2018. These include logging requirements, categorisation and obligations about the principles and rights of individuals.

Example

A Police force is dealing with an internal disciplinary matter involving a member of staff. A complaint has been referred to a professional standards department about an officer's conduct. The complaint is not of a criminal matter.

The processing involves the use of data from various internal sources, such as HR. The primary purpose for processing the data is to investigate staff conduct and behaviour, so will be processed under the general processing regime.

As the investigation progresses, an element of criminality is discovered. The relevant data is then passed to a specific team. They will process the data to investigate the criminal aspects, so will need to comply with the law enforcement processing regime under Part 3 of the DPA 2018.

The HR department may still be processing some of the data for HR-related matters, and that will still be processed under the general processing regime.

Further reading

Read our guidance on:

Data sharing and reuse of data by competent authorities for non-law enforcement purposes

How is personal data defined?

Any information relating to an identified or identifiable **living** individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only be potentially linked to a living individual.

Further Reading

Relevant provisions in the Act - See Section 1
External link

What is a controller?

A controller determines how and why personal data is processed. For the purposes of law enforcement, this will be a competent authority which is acting alone, or jointly with others.

If you are processing jointly with another competent authority, you must designate a specific controller to be the contact point for data subjects.

If you are a processor, you are processing personal data on behalf of the controller for the law enforcement purposes, but you could be sharing some accountability with controllers. This means that you could be liable for breaches. You need to review and revise your contracts to ensure that they reflect your new obligations.

Further Reading

Relevant provisions in the Act - See Section 32
External link

What is sensitive processing?

Sensitive processing is defined in section 35(8) 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, or of biometric data, for the purpose of uniquely identifying an individual;
>
> (c) the processing of data concerning health;
>
> (d) the processing of data concerning an individual's sex life or sexual orientation.

Genetic data is personal data relating to the inherited or acquired characteristics of a person, eg an analysis of a biological sample.

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.

For more information on the rules about sensitive processing, see our guide pages on the principles and conditions for sensitive processing.

Further Reading

Relevant provisions in the Act - See Sections 35 and 205
External link

Principles

At a glance

- The six law enforcement data protection principles under Part 3, Chapter 2 of the DPA 2018 are the main responsibilities you should follow when processing personal data for law enforcement purposes.
- The principles are broadly the same as those in the UK GDPR, and are compatible so you can manage processing across the two regimes.
- There are no principles relating to individuals' rights or overseas transfers of personal data – these are addressed in Part 3 of the DPA 2018 separately.
- Transparency requirements are not as strict as in the UK GDPR, due to the potential to prejudice an ongoing investigation in certain circumstances.
- You must be able to demonstrate overall compliance with all of the law enforcement data protection principles.

In brief

What are the principles?

Part 3, Chapter 2 of the DPA 2018 sets out six key principles which are your main responsibilities when processing personal data for the law enforcement purposes.

The principles are broadly the same as those in the UK GDPR, and are compatible so you can manage your processing across the two regimes.

The first data protection principle

Processing of personal data for any of the law enforcement purposes must be lawful and fair.

The second data protection principle

The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;

Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

The third data protection principle

Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The fourth data protection principle

Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;

Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

The fifth data protection principle

Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

The sixth data protection principle

Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Section 34(3) adds that:

> The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.

Why are the principles important?

The principles guide and inform the processing of personal data for the law enforcement regime under Part 3 of the DPA 2018.

They don't give hard and fast rules, but rather embody the spirit of the law enforcement regime – and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of Part 3.

Failure to comply with the principles may leave you open to substantial fines. Section 157(2)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of monetary penalties. This could mean a penalty of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

What is the first principle about?

The first data protection principle says that any processing for the law enforcement purposes must be lawful and fair. Lawfulness and fairness are well established requirements of data protection law.

For the processing to be lawful, section 35(2) says that it must be "based on law". This means that the processing is authorised by either statute, common law or royal prerogative, or by or under any other rule of law. You must identify a legal basis that provides a sufficiently clear, precise and foreseeable lawful justification to process personal data for the law enforcement purposes. The necessary legal basis may be found in more than one statute or other source of law.

Example

Part 5 of the Police and Criminal Evidence Act 1984 confers statutory authority for the taking and retention of DNA and fingerprints (this applies to England and Wales).

The Domestic Violence Disclosure Scheme relies on the Police's common law powers to disclose information where it is necessary to do so to prevent crime.

The processing must also have a lawful basis under data protection legislation. Section 35(2) explains that

the processing of personal data for any of the law enforcement purposes must be either necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent.

You need to be aware that any processing you carry out for the law enforcement purposes must be necessary. This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving your purpose. This lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate in a particular way. The question is whether the processing is a necessary for the stated purpose.

In terms of consent under Part 3, this has the same high standard of consent as that in the UK GDPR. This means consent must be freely given and it must be unambiguous and involve a clear affirmative action (an opt-in). Individuals also must be able to easily withdraw consent. Further guidance on consent can be found in the Guide to UK GDPR page.

There may be limited circumstances where you obtain consent from the individual whose personal data you are processing. However, in the context of law enforcement processing, consent may often not be appropriate as a lawful basis.

"Fairness" generally means you must not process personal data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. It also requires you to be, where appropriate, clear and open with individuals about how you use their information, in keeping with their reasonable expectations.

What about sensitive processing?

In the context of law enforcement, the personal data you are processing will often be sensitive. When it is, you must be able to demonstrate that the processing is **strictly necessary** and satisfy one of the conditions in Schedule 8 of the DPA 2018, or is based on consent. Strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means. This is a requirement which will not be met if you can achieve the purpose by some other reasonable means.

Sensitive processing is defined in the law enforcement provisions 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, or of biometric data, for the purpose of uniquely identifying an individual;
>
> (c) the processing of data concerning health;
>
> (d) the processing of data concerning an individual's sex life or sexual orientation.

Genetic data is personal data relating to the inherited or acquired characteristics of a person, eg an analysis of a biological sample.

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

Given the sensitivity surrounding such processing, you are required to meet at least one of the conditions set out in Schedule 8 of the DPA 2018.

What safeguards are required for sensitive processing?

If you are carrying out sensitive processing based on the consent of a data subject, or based on another specific condition in Schedule 8 of the DPA 2018, you must have an appropriate policy document in place.

This document must explain:

- your procedures for ensuring compliance with the law enforcement data protection principles; and
- your policies on the retention and erasure of this data.

You must retain this policy from the time you begin sensitive processing until six months after it has ended. You must review and update it where appropriate and make it available to the Information Commissioner upon request without charge.

So, to recap, sensitive processing must be:

- based on the consent of the data subject; or
- strictly necessary for the law enforcement purpose and based on a Schedule 8 condition.

In addition, in either case you must have an appropriate policy document in place.

Our template appropriate policy document shows the kind of information this should contain.

What is the second principle about?

The second principle is about maintaining the purpose for processing personal data. Specific requirements about the purpose being **specified, explicit and legitimate** are introduced, meaning that any processing under Part 3 of the DPA 2018 must be for the defined law enforcement purposes. You cannot process for a purpose that is incompatible with the original reason and justification for processing.

> The Crown Prosecution Service could process personal data in connection with the prosecution of a criminal offence, whereas the Police working alongside the prosecutor would only be processing the personal data in connection with the investigation of the offence.

What are principles three, four and five about?

The third principle requires that the personal data you are processing is **adequate, relevant and not excessive**. This means the data must be limited to what is necessary for the purpose(s) you are processing it.

The fourth data protection principle is about accuracy. It sets out that you should take every reasonable step to correct inaccurate data. In addition, **as far as possible**, you need to be able to distinguish between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

A new requirement is that again, where relevant, and as far as possible, you need to be able to distinguish data between different categories of individuals, such as suspects; individuals who have been convicted; victims and witnesses. You only categorise information under Part 3 that is relevant to your investigation, and other unused data falls under the general processing regime.

The fifth principle requires that you do not keep personal data for longer than is necessary for the purpose you originally collected it for. No specific time periods are given but you need to conduct regular reviews to ensure that you are not storing for longer than necessary for the law enforcement purposes.

What is the sixth principle about?

The sixth principle requires you to have technical and organisational measures in place to ensure that you protect data with an appropriate level of security. This is the same as under the UK GDPR and Part 2 of the DPA 2018

"Appropriate security" includes "protection against unauthorised or unlawful processing and against accidental loss, destruction or damage".

Further Reading

> Relevant provisions in the DPA 2018 - see Sections 34,35, 36, 37, 38, 39, 40, 41, 42, 157 and Schedule 8
> External link

Conditions for sensitive processing

At a glance

The conditions for sensitive processing in Schedule 8 of the Act are:

- necessary for judicial and statutory purposes – for reasons of **substantial public interest**;
- necessary for the administration of justice;
- necessary to protect the vital interests of the data subject or another individual;
- necessary for the safeguarding of children and of individuals at risk;
- personal data already in the public domain (manifestly made public);
- necessary for legal claims;
- necessary for when a court acts in its judicial capacity;
- necessary for the purpose of preventing fraud; and
- necessary for archiving, research or statistical purposes.

Again, you must be able to demonstrate that the processing is **strictly necessary** and satisfy one of the conditions in Schedule 8 or is based on consent. Strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means.

In brief

What are the conditions?

When undertaking 'sensitive processing', in order to comply with the first principle, you must either have consent for processing or be able to satisfy one of the conditions in Schedule 8. Consent should not always be a default condition as it may not be appropriate in the circumstances. You will also need an appropriate policy document in place.

What is an appropriate policy document?

An appropriate policy document must explain:

(a) your procedures for ensuring compliance with the law enforcement data protection principles; and

(b) your policies on the retention and erasure of this data.

Our template appropriate policy document shows the kind of information this should contain.

What are judicial and statutory purposes/administration of justice?

The sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities.

In addition, in order to satisfy this condition, you must be able to demonstrate that the processing is necessary for reasons of substantial public interest.

When is processing appropriate for individual's vital interests?

This condition only applies in cases of life or death, such as if you disclose an individual's medical history to a hospital's A&E department who are treating them after a serious road accident. Data protection law should not be a barrier to processing data in these circumstances.

When does processing relate to safeguarding of children and of individuals at risk?

This condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest, and is to protect them from harm or to protect their well-being.

What about personal data already in the public domain?

This condition applies if the data subject has deliberately made the information public.

What about legal claims and judicial acts?

This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity.

When can data be processed for preventing fraud?

You should use this condition if the processing is necessary for the purposes of preventing fraud. If it involves sharing data with organisations that do not fall within the definition of a competent authority, the processing needs to comply with the UK GDPR, and you need to have a lawful basis for sharing the data.

What about archiving?

You can use this condition if processing is necessary for archiving in the public interest; for scientific or historical research purposes, or for statistical purposes. However, you cannot use it if it will result in decisions being made that effect a particular individual, or is likely to cause substantial damage or

substantial distress to an individual.

Further Reading

Relevant provisions in the Act - See Schedule 8
External link

Individual rights

Part 3, Chapter 3 of the Act provides the following individual rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restrict processing; and
- the right not to be subject to automated decision-making.

Certain rights under the UK GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights.

It is important to note that subject access rights and the rights to rectification, erasure and restriction do not apply to the processing of **'relevant personal data'** in the course of a criminal investigation or criminal proceedings.

'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.

Access to 'relevant personal data' is governed by the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigations Act 1996.

This provision only applies if the judge or other judicial authority is the controller and the relevant personal data is contained in a judicial decision or in other documents which are created during a criminal investigation or proceedings and made by or on behalf of the judge or judicial authority. For example, the 'relevant personal data' may be contained in judge's notes.

You must communicate any information in clear and plain language that you are required to provide in Part 3. It is also your duty more generally to assist individuals to exercise their rights.

Similar to the UK GDPR, the Act includes further provisions for individuals to exercise their rights through raising a complaint with the Information Commissioner, or taking matters to court.

The next sections explain each of these in more detail.

The right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data;
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information';
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language;
- Exemptions apply, and you may restrict the provision of information where it is necessary and proportionate.

In brief

How should we provide this information?

The information you supply about the processing of personal data must be:

- concise, intelligible and easily accessible;
- written in clear and plain language, adapting this to the needs of vulnerable persons, such as children; and
- free of charge.

What information must we supply as a minimum?

You must make this information generally available to the public:

- your identity and contact details;
- the contact details of your data protection officer, if applicable;
- purposes of the processing;
- the individual's rights (access, rectification, erasure and restriction); and
- the right to lodge a complaint with the Information Commissioner and the contact details of the ICO.

What information should we supply to an individual?

You should supply the following information to enable an individuals to exercise their rights:

- your legal basis for processing;
- your retention period or the criteria you used to determine the retention period;
- any recipient or categories of recipients of the personal data (including in third countries or international organisations); and
- any further information needed to enable individuals to exercise their rights, eg if information is collected without their knowledge

The right to this information is a qualified right, subject to restrictions that prevent any prejudice to an ongoing investigation or compromise to operational techniques.

Example

You have a generic privacy notice on your website which covers basic information about the organisation, the purpose you process personal data for, a data subject's rights and their right to complain to the Information Commissioner.

You have received intelligence that an individual was present when a crime took place. On first interviewing this individual, you need to provide the generic information, as well as the further supporting information, to enable their rights to be exercised. You can only restrict the fair processing information you are providing if it will adversely affect the investigation you are undertaking.

In what circumstances may we limit the provision of further supporting information?

You may restrict the provision of further information where it is necessary and proportionate to:

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

You need to justify any restriction you apply as necessary and proportionate, and apply it on a case by case basis. It is important to balance the rights of the individual against the harm disclosure would cause.

You also must inform the individual when this limitation is in place, explaining its existence and the reasons, unless providing this information itself will undermine the purpose of imposing the restriction. Regardless, you still need to inform the individual about the process of raising a complaint with the Information Commissioner or taking matters to court.

You should keep a record of your decisions to rely on any restriction, and provide this reasoning to the Information Commissioner if required.

Further Reading

Relevant provisions in the Act - See Section 44, Chapter 3
External link

The right of access

At a glance

- Individuals have the right to be aware of and verify the lawfulness of the processing you are carrying out.
- There is no requirement for a request to be in writing. Therefore, it is good practice to have a policy for recording details of all the requests you receive, including verbal requests.
- You must provide a copy of the information free of charge.
- You must provide the information requested without delay and at the latest within one month of receipt.

In brief

What is the purpose of the right of access under Part 3 of the Act?

Individuals have the right to access their personal data and supplementary information, subject to certain restrictions.

This right allows individuals to be aware of and verify the lawfulness of the processing you are carrying out.

What do we need to do to comply with a request?

There is no requirement for a request to be in writing. Therefore, it is good practice to have a policy for recording details of all the requests you receive. We also recommend that you keep a log of verbal requests as these will also be considered as a valid request.

You may wish to check with the requester that you have understood their request as this can help avoid later disputes.

If you have reasonable doubts about the identity of an individual, you can request more information to confirm it. This is particularly important when you are handling sensitive data. You can delay dealing with the request until you receive further information to establish their identity.

Your request for information to verify a requester's identity should be reasonable and proportionate, taking

into consideration the nature of the personal data you hold and your relationship with the individual.

What information is an individual entitled to?

When your processing is for the law enforcement purposes, individuals have the right to obtain confirmation that you are processing their data, and if so:

- access to their personal data; and
- other supplementary information – this largely aligns with the information that should be provided in a privacy notice but includes the categories of personal data concerned, information about its origin, and the right to raise a complaint with the Information Commissioner.

Unlike the UK GDPR, where you can contact the individual to clarify the request if it involves a large amount of personal data, there is no similar provision under Part 3 of the Act. In practice, you may need to contact the requester to clarify the request but this will fall within the timescale for responding to the request.

What information do we need to provide in response to a request?

An individual is entitled to the following information:

- your purposes for processing and the legal basis you are relying on;
- categories of personal data you're processing;
- recipients or categories of recipients you are disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- your retention period, or your criteria for determining this;
- their rights to request rectification, erasure or restriction;
- their ability to raise a complaint with the Information Commissioner and the ICO's contact details; and
- the personal data you are processing (in writing) and any available information you have about the origin of the data.

Remember, the information you supply about the processing of personal data must be:

- concise, intelligible and easily accessible; and
- written in clear and plain language, adapting this to the needs of vulnerable persons, such as children.

Where possible, you should provide the information in the same form in which the request was made. For instance, you should respond to a request by email through the same means unless the volume of information makes this prohibitive.

Can we charge a fee for dealing with a subject access request?

You must provide a copy of the information free of charge.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information (the month starts after you've received the fee); or

- refuse to respond.

It will be for you, the data controller, to determine what is manifestly unfounded or excessive. However, you will have to demonstrate to the Information Commissioner why you have decided that a request is manifestly unfounded or excessive if asked, and maintain a record of this decision making.

How long do we have to comply with a subject access request?

You must provide the information requested without delay and at the latest within one calendar month, from the first day after the request was received.

Example

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

For practical purposes if a consistent number of days is required (eg for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

If you require further information to establish the identity of a requester, the month will start when you have received this.

Unlike the UK GDPR, you are not able to extend the period of compliance by a further two months if requests are complex or numerous.

What if the data involves third party personal data?

You can restrict the amount of personal data you supply when it is necessary and proportionate to "protect the rights and freedoms of others." If information contains the personal data of an individual and that of third parties, you have to consider whether it is reasonable to disclose this information and whether this would adversely affect the rights and freedoms of others. You may need to consider redacting it, and record any reasons for withholding such information from disclosure.

When can we restrict the amount of information we provide?

You may limit the following information (in full or in part):

- confirmation that you are processing data; and
- access to personal data.

if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;

- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

You need to justify any restriction you apply as necessary and proportionate. It is important to balance the rights of the individual against the harm disclosure would cause. You may only limit the amount of information you provide if it would prejudice the purposes stated above.

You must also inform individuals when this limitation is in place, explaining the existence and the reasons, unless providing this information itself undermines the purpose of imposing the restriction. You also need to inform them about the process for raising a complaint with the Information Commissioner or taking matters to court.

You should keep a record of your decisions and provide this reasoning to the Information Commissioner, if required.

Example

An individual you are investigating for tax fraud makes a request for all their personal data that you hold. You can only restrict the amount of personal data you provide in so far as disclosing it will prejudice an active investigation. P45 forms, or records on the individual's income which were self-reported for instance, are information they are aware of and therefore withholding it is likely to be unjustified. However you can clearly restrict access to investigative files and evidence which you have gathered.

In this case, you do not have to notify the individual that you have restricted their right of access, as this is likely to alert them to your investigation.

Providing a written copy of personal data you processed is only complying with part of the right. You also have to provide other information required such as the legal basis for processing and retention period, unless by providing this information will again prejudice an investigation.

There should not be a blanket application of any exemption. Instead, you have to assess individual items of personal data you hold to decide whether disclosure will prejudice an ongoing investigation.

Further Reading

Relevant provisions in the Act - See sections 45, 51, 54 and Chapter 3
External link

The right to rectification

At a glance

- Individuals have the right to have personal data rectified.
- You can rectify personal data if it is inaccurate or incomplete.
- You must rectify any inaccurate personal data that relates to the individual without undue delay, and in any event within one month.

In brief

When should we rectify personal data?

You must rectify inaccurate personal data when it becomes apparent, or, if an individual requests it. If personal data is identified as inaccurate as a matter of fact, or incomplete, you must seek to amend this by rectifying or completing the data. If you are unable to correct it, you could provide a supplementary statement to rectify personal data which is inaccurate if appropriate. In circumstances such as policing, you can keep accurate records of allegations made, even if the allegations are unfounded.

Example

The right to rectification applies, in particular, to matters of fact. For example, there may be inaccuracies in the details of a criminal conviction held on the Police National Computer. An individual may receive a copy of their criminal record and request that an incorrect entry for Grievous Bodily Harm is corrected to Actual Bodily Harm, or vice versa, to reflect the correct conviction. The controller may restrict the right to rectification if, for example, it obstructs an investigation, such as a request to rectify the content of a witness statement.

If you need to maintain personal data for the purposes of evidence, you must restrict its processing (instead of rectifying it). There is further information in the next section about restricting the processing of personal data.

If this happens, an individual may raise a complaint with the Information Commissioner.

What do we need to do to comply?

An individual can make a request for rectification verbally or in writing. Therefore, it is good practice to have a policy for recording details of the requests you receive, including those made by telephone or in person. You may wish to check with the requester that you have understood their request as this can help avoid later disputes. We also recommend that you keep a log of verbal requests.

If you have reasonable doubts about the identity of an individual, you can request more information to confirm their identity. You can put dealing with the request on hold until you receive further information to establish their identity.

Your request for verification should be reasonable and proportionate, taking into consideration the nature of the personal data you hold and your relationship with the individual.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification. The third parties also have to rectify the information they hold. You must also inform the competent authority (if any) where the inaccurate personal data originated from.

If you refuse a request for rectification, you must tell the individual, informing them of their right to raise a complaint with the Information Commissioner or taking matters to court.

What if the request is manifestly unfounded or excessive?

If requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

You have to be able to demonstrate how a request is manifestly unfounded or excessive.

How long do we have to comply?

You must respond to the request without delay and at the latest within one calendar month, from the first day after the request was received.

Example

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

For practical purposes if a consistent number of days is required (eg for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

When can we limit the provision of information?

If you receive a request for rectification, you must inform the individual in writing whether you have granted the request; and if you have refused, the reasons why, as well as the process for raising a complaint with the Information Commissioner or taking matters to court.

You may limit the provision of information to:

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

You need to justify any restriction you apply as necessary and proportionate. Again, you should also consider whether refusal or rectification in itself prejudices an ongoing investigation, as it may well indicate to an individual that you are processing their personal data.

You still need to inform the individual about their right to raise a complaint with the Information Commissioner or take matters to court.

In addition, you should keep a record of your decisions and provide this reasoning to the Information Commissioner, if required.

Further Reading

Relevant provisions in the Act - See sections 46, 48, 52 and 53, Chapter 3
External link

The right to erasure and the right to restriction

At a glance

- Individuals also have the right to request the deletion or removal of their personal data.
- Individuals also have a right to 'block' or restrict processing of their personal data.

In brief

The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals also have the right to restrict the processing of their personal data.

The Act defines the restriction of processing as the 'marking of stored personal data with the aim of limiting its processing for the future'.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that you respect the restriction in future.

Restriction could involve measures such as transferring data to a separate system, or limiting the access through the use of passwords and other access controls.

What do we need to consider when deciding if the right to erasure applies?

Individuals have a right to have personal data erased or to restrict its processing.

You must erase personal data without undue delay if:

- the processing of the personal data will infringe **the data protection principles**;
- you do not meet safeguards for **archiving** and processing of **sensitive personal data**; or
- you have a **legal obligation** to erase the data.

We recognise that complete deletion of personal data in electronic systems can often be problematic, but you should ensure that you have adequate systems and storage media in place to comply with an individual's request for erasure. If deletion is not technically possible, you should at least take steps to put the personal data 'beyond use'.

What do we need to do to comply with requests for erasure or restriction?

The Act does not specify how to make a request, so an individual can do so verbally or in writing. Therefore, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request as this can help avoid later disputes. We also recommend that you keep a log of verbal requests.

If you have reasonable doubts about the identity of an individual, you can request more information to confirm their identity. You can delay dealing with the request until you receive further information to establish their identity.

Your request for information to verify a requester's identity should be reasonable and proportionate, taking into consideration the nature of the personal data you hold and your relationship with the individual.

If you have disclosed the personal data in question to third parties, you must inform the third party about the erasure or restriction of the personal data. The third parties will also have to erase or restrict the personal data they hold.

You must tell an individual if you are not going to erase or rectify the personal data they have requested that you amend. You must also inform them of their right to raise a complaint with the Information Commissioner or take the matter to court.

What if the request is manifestly unfounded or excessive?

If requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

You have to be able to demonstrate how a request is manifestly unfounded or excessive.

How long do we have to comply?

You must respond to the request without delay and at the latest within one calendar month, from the first day after the request was received.

Example

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

For practical purposes if a consistent number of days is required (eg for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

When should we restrict processing?

You are required to restrict the processing of personal data for the law enforcement purposes in two situations:

- If you must maintain personal data for the purposes of evidence.
- If an individual contests the accuracy of personal data but it is not possible to be certain about its accuracy.

If restriction is based on the latter, you should inform the individual before you lift the restriction.

Example

A local authority is investigating a suspect for benefit fraud. As part of this investigation, factually inaccurate personal data about the suspect (such as an age/ethnicity) has been received from a third party. However this inaccurate record needs to be retained as evidence to account for how the local authority first carried out the investigation and the source of this information. They should not erase or rectify this information, but restrict it as it forms evidence against the suspect. They should not process this inaccurate personal data for any other purpose.

When can we limit the provision of information?

If you receive a request for rectification, you must inform the individual in writing whether you have granted the request; and if you have refused, the reasons why, as well as the process for raising a complaint with the Information Commissioner or taking matters to court.

You may limit the provision of information where it is necessary and proportionate to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the

execution of criminal penalties;

- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

Any restriction you apply needs to be justified as necessary and proportionate. In deciding on proportionality it is important to balance the rights of the data subject against the harm disclosure would cause. You can only limit the information you provide to the extent that it would prejudice the purposes stated above.

There is also an obligation to inform the data subject when this limitation is in place, explaining its existence and the reasons unless providing this information itself undermines the purpose of imposing the restriction. You still need to inform the individual about recourse to the Information Commissioner and the Court process.

You should keep a record of your decisions and provide this reasoning to the Information Commissioner if required.

Further Reading

> Relevant provisions in the Act - See sections 47, 48, 52 and 53, Chapter 3
> External link

Right not to be subject to automated decision-making

At a glance

- Part 3 provides safeguards for individuals against the risk that a potentially damaging decision is taken by **solely** automated means, ie without human intervention.
- You may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. A 'qualifying significant decision' is defined as a decision which significantly affects or produces an adverse legal effect on an individual and is authorised by law.
- Currently, solely automated decision-making that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have many operational implications.

In brief

When does the right apply?

Individuals have the right **not to be subject to a decision** when:

- it is based on automated processing; and
- it produces an adverse legal effect or significantly affects the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

To qualify as human intervention, you must ensure that you carefully analyse the decision and consider all the available input and output data, rather than just a token review. This should be carried out by someone who has the authority and competence to change the decision.

This right does not specifically refer to profiling. However, profiling is defined in section 33 as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- interests;
- reliability;

- behaviour;
- location; or
- movements.

Profiling and automated decision-making can be combined activities of the same process, or can be carried out separately. There may be cases of automated decisions made with (or without) profiling and profiling which may take place without making automated decisions. This right will therefore apply to any profiling which involves some form of automated processing.

The right does not apply when a decision does not have an adverse legal or similarly significant effect on someone.

Example

An automated processing system could include an IT database of criminal records or prosecution histories, where data is input or accessed by staff via automated means.

'Automated decision making' only comes into play where the controller takes a 'significant' decision based solely upon automated processing, often without any human interaction. This is a decision that produces an adverse legal effect concerning the individual or otherwise affects the individual.

How do we comply?

You should inform an individual if you make a 'qualifying significant decision' about them.

The individual has one month to request for you to review the decision, or take a new decision not based solely on automated means. You must consider the request including any information provided by the individual. You need to respond to the individual within one month of receipt of their request and outline the steps you have taken as well as the outcome.

The DPA 2018 does not specify how an individual must make a request, so they can make it verbally or in writing. Therefore, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes.

Further Reading

Relevant provisions in the DPA 2018 - See Sections 49, 50, 52 and 53, Chapter 3
External link

Other resources

Toolkit for organisations considering using data analytics

Manifestly unfounded and excessive requests

At a glance

- Under Part 3 of the DPA 2018 individuals have rights of access, rectification, erasure or restriction, and to not be subject to automated decision-making.
- You may refuse to respond to a request if it is manifestly unfounded or excessive.
- Alternatively you may charge a reasonable fee for dealing with the request.
- You must be able to demonstrate why it is manifestly unfounded or excessive.

In brief

How should we respond to manifestly unfounded and excessive requests?

If you process personal data for law enforcement purposes, you may refuse to respond to certain requests from individuals if you can demonstrate that they are **manifestly unfounded** or **excessive.**

Alternatively, you may choose to respond to a request that you regard as manifestly unfounded or excessive. If so, you may charge a reasonable fee for doing so.

You should not have a blanket policy for determining whether a request is manifestly unfounded or excessive. You must consider each request on a case-by-case basis.

Whilst there may be characteristics that are indicative of a manifestly unfounded or excessive request (please see the next sections), you should only use these as a guide. Also, you should not presume that a request is manifestly unfounded or excessive just because the individual has previously submitted requests which have been manifestly unfounded or excessive.

You must be able to demonstrate to the individual why you consider the request is manifestly unfounded or excessive and, if asked, to the Information Commissioner.

What does manifestly unfounded mean?

A request may be manifestly unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption.

Factors that may indicate malicious intent include:

- the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated accusations against you or specific employees;
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.

These factors are not intended to form a simple tick list that automatically mean a request is manifestly unfounded. You must consider a request in the context in which it is made, and the onus on you is to be able to demonstrate it is manifestly unfounded.

The inclusion of the word "manifestly" means it must be obvious or clear that it is unfounded. You should consider the particular situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request is manifestly unfounded. In most cases, use of aggressive or abusive language does not, in itself, demonstrate a manifestly unfounded request.

Example

An individual believes that information held about them is inaccurate. They repeatedly request its correction but you have previously investigated and told them you regard it as accurate.

The individual continues to make requests along with unsubstantiated claims against you as the controller.

You refuse the most recent request because it is manifestly unfounded and you notify the individual of this.

What does excessive mean?

Whether a request is excessive depends on its particular circumstances. A request may be excessive if it:

- repeats the substance of previous requests and a reasonable interval has not elapsed; or
- overlaps with other requests.

You must still try to comply with a large request by making **reasonable** searches for the information. While requests will be handled on a case by case basis, in the interest of good practice, you must ensure you have appropriate records management procedures in place to handle large requests and locate information efficiently.

In most cases, a request is not excessive just because the individual has asked for a large amount of information, even if you find it a burden. You can ask them for more information to help you locate the information they want to receive.

Requests about the same issue are not always excessive. An individual may have legitimate reasons for

making requests that repeat the content of previous requests. For example, if the controller has not handled previous requests properly.

An individual may also want to receive another copy of information they have requested previously. In this situation a controller can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this is an excessive request.

A repeat request may also not be excessive if a reasonable amount of time has passed since their last request. In deciding whether a reasonable interval has elapsed, you should consider:

- the nature of the data – this could include whether it is particularly sensitive, but also the value of the information to the individual;
- the purposes of the processing – these could include whether the processing is likely to cause harm to the requester if disclosed;
- how often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this; and
- remember, this is not just about the right of subject access. You should also consider the importance of individuals being able to exercise the other rights that apply.

A request may be excessive if an individual makes a new request before you have had the opportunity to address an earlier request. However, this is only the case if the substance of the new request repeats some of the previous request. It is unlikely to be excessive, if the overlapping request is about a completely separate set of information.

What should we do if we refuse to comply with a request?

If you refuse to comply with a request you must inform the individual about:

- the reasons why you have not complied with their request;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

As mentioned above, if you believe a request is manifestly unfounded or excessive you must be able to demonstrate this to the individual. If an exemption applies, the reasons you give to an individual for not complying with their request may depend on the particular case. For example, if telling an individual that you have applied a particular exemption would prejudice the purpose of that exemption, your response may be more general. However, if it is appropriate to do so, you should be transparent about your reasons for withholding information.

When can you charge a fee?

Under Part 3 of the DPA 2018, you can no longer request a fee for processing a subject access request. However, you may charge a reasonable fee if you decide that a request to exercise a right under sections 45, 46, 47 or 50 is manifestly unfounded or excessive, but you still choose to respond to it.

If you do decide to charge a fee, you should notify the requester and say why. You do not need to send the information or respond to the request until you have received the fee. The time limit for responding to the

request begins once the requester has paid the fee.

If you decide on a reasonable fee, you must be able to justify the cost, in case the requester makes a complaint to the Information Commissioner.

Example

An individual repeatedly requests a personal file through the right of access. You have given them the same file before, but you decide to respond to the request because you think they may have lost the file and it is harmful for them not to have this information.

You tell the individual you are charging them a fee for this information, based on the cost of administration. Once you have received the fee, you provide the information within one calendar month.

Further Reading

Relevant provisions in Part 3 of the DPA 2018 - See Chapter 3, section 53
External link

Accountability and governance

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are legally required in certain circumstances that pose a risk to the rights and freedoms of individuals.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many will already have good governance measures in place.

What is the accountability principle?

Part 3, Chapter 2 of the Act requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility as data controller.

How can we demonstrate that we comply?

You must implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

In addition, you must:

- maintain relevant documentation on your processing activities;
- where appropriate, appoint a data protection officer; and
- implement measures that meet the principles of data protection by design and data protection by default.

Such measures could include:

- data minimisation;
- pseudonymisation;
- transparency, where appropriate;
- creating and improving security features on an ongoing basis; or
- data protection impact assessments where appropriate.

Further Reading

Toolkit for organisations considering using data analytics

For organisations

Documentation

At a glance

- You must maintain internal records of processing activities.
- If a processor is acting on your behalf, the processer must also maintain a record of processing activities they are carrying out.
- You and any associated processor may be required to make these records available to the Information Commissioner on request.

In brief

What do I need to record?

You must maintain internal records of processing activities including:

- your name and details (and where applicable those of other controllers, your representative and data protection officer);
- purposes of your processing;
- description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- your retention schedules; and
- a description of your technical and organisational security measures.

If a processor is acting on your behalf, the processer must also maintain a record of processing activities they are carrying out including:

- the name and contact details of the processor (and where applicable, of other processors, their representative and data protection officer);
- the categories of processing carried out on your behalf;
- details of transfers to third countries where explicitly instructed, including documentation of the transfer mechanism safeguards in place and identification of that third country; and
- a description of technical and organisational security measures.

You and any associated processor may be required to make these records available to the Information Commissioner on request.

Further Reading

Relevant provisions in the Act - See sections 61, Chapter 4
External link

Logging

At a glance

If you operate automated processing systems (any IT database), you must keep logs for **at least** the following processing actions:

- Collection
- Alteration
- Consultation
- Disclosure (including transfers)
- Combination
- Erasure

In brief

What is the purpose of logging?

It is to enable you to monitor and audit internal processing within any automated processing systems you use, and to know which third parties you have shared data with so that you can inform them of changes to the data should you need to. In addition, logging enables you to monitor systems for inappropriate access and/or disclosure of data, to verify the lawfulness of any processing, and to ensure the integrity and security of personal data.

> **Example**
>
> If an officer or member of police staff is suspected of inappropriately accessing the Police National Computer to check on a neighbour, family member or friend, the logging should show what was available to them at the time, which will assist with any potential internal investigations.

The law enforcement provisions do not include a definition of 'automated processing system' however it is interpreted to mean any system that undertakes processing by automated means, and is likely to involve human interaction (for example input of or access to data) at some point.

If you operate automated processing systems (any IT database), you must keep logs for **at least** the following processing actions:

- Collection
- Alteration
- Consultation

- Disclosure (including transfers)
- Combination
- Erasure

It is important that you do not record the data itself in your logs of erasure, as there is no need to retain a duplicate record of what you have erased. The requirement is to produce metadata which displays, for example, what a specific person on a specific date erased. The 'what' does not have to detail the content of the record/information that has been deleted – it can simply record that record *X* was updated by a specific individual.

Logs must also record, where possible, the identity of the person who accessed (consulted) the data, the reason for the access, and the date and time of any associated action. You should also record the identity of any recipients, in cases of disclosure – this is particularly important as you will need to inform the recipients if you delete, amend or restrict the processing of this data following a request from the individual.

There are however limitations to what you can use logs for. Any logs that you keep for the above processing actions may only be used for one or more of the following purposes:

- to verify the lawfulness of processing;
- to assist with self-monitoring by the controller or the processor, including the conduct of internal disciplinary proceedings;
- to ensure the integrity and security of personal data; or
- the purposes of criminal proceedings.

You (and any associated processor) may be required to make these records available to the Information Commissioner upon request.

Further Reading

> Relevant provisions of the Act - See section 62, Chapter 4
> External link

Categorisation of individuals

At a glance

When processing personal data for the any of the law enforcement purposes, you must provide, **where relevant and as far as possible**, a clear distinction between different categories of personal data, such as people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;
- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

In brief

Under the fourth principle, you must ensure that any personal data you process for law enforcement purposes is accurate and, where necessary, up to date.

In all areas of policing and criminal justice, it is highly likely that any processing of personal data will involve different categories of data subject. When processing personal data for the any of the law enforcement purposes, you must provide, **where relevant and as far as possible**, a clear distinction between different categories of personal data, such as people who are:

- suspected of having committed, or about to commit, a criminal offence (suspects);
- convicted of a criminal offence;
- individuals who are, or are suspected of being, victims of a criminal offence (victims); or
- individuals who are witnesses, or can provide information, about a criminal offence (witnesses).

There may be instances where an individual falls under more than one of these categories. For example an individual may be both a victim and a witness in a certain case, or indeed an offender in one case and victim/witness in another. You will therefore be required, where relevant and as far as possible, to have processes and procedures in place to distinguish between such categories.

Example

If a competent authority obtains a large dataset as part of an investigation, the authority only needs to categorise the personal data that is relevant to the investigation. In practice, this will be data that has operational value to a criminal investigation, rather than any other collateral data that they have also acquired.

The competent authority will only categorise the information under Part 3 **where relevant** to the investigation, and any other unused data will fall under the general provisions of the UK GDPR/ Part 2 of the Act.

It is important to note that any unused personal data is also subject to strict retention periods.

You must also distinguish, so far as possible, any personal data based on facts from personal data based on personal assessment. In essence, this is the ability to distinguish between fact and opinion.

For example, statements by victims and witnesses containing personal data are based on the subjective perceptions of the person making the statement. These statements are not always verifiable and are subject to challenge during the legal process. In such cases, the requirement for accuracy does not apply to the content of the statement but simply that a specific statement has been made.

The requirement to keep personal data up to date must also be viewed in this context. If an individual's conviction is overturned on appeal, police must amend their records. However, they will not retrospectively alter a witness statement even if the court has found it to be unreliable.

Further Reading

Relevant provisions of the Act - See Section 38, chapter 2
External link

Data protection by design and by default

At a glance

- You have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.
- Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.
- The ICO has published guidance on privacy by design and default within the Guide to the UK GDPR.

In brief

What is data protection by design?

Under the UK GDPR and Part 3 of the Act, you have a general obligation to implement appropriate technical and organisational measures to show that you have considered and integrated the principles of data protection into your processing activities.

If you are processing personal data for law enforcement purposes, you must implement these measures by default, to ensure that you only process personal data for a specified and necessary purpose.

In particular, you must ensure that by default, you put safeguards in place to prevent personal data being made available to an indefinite number of people without an individual's intervention.

Example

An authority responsible for courts and tribunals are building new IT systems for storing or accessing personal data. Prior to any live use, the authority is required to review their privacy and data protection compliance and perceived risks from the start of the project, rather than adding on such considerations at the end. This process could involve undertaking a Data Protection Impact Assessment (DPIA).

Further Reading

Relevant provisions of the Act - See Section 57, Chapter 4
External link

Data protection impact assessments

At a glance

- A data protection impact assessment (DPIA) is 'an assessment of the impact of the envisaged processing operations on the protection of personal data'.
- You must carry out a DPIA before you process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- The ICO has produced guidance and screening checklists about DPIAs that you may wish to adopt.

In brief

What is a data protection impact assessment?

Data protection impact assessments or DPIAs (previously known as privacy impact assessments or PIAs) are a tool that can help you identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

When do we need to conduct a DPIA?

You must carry out a DPIA before you process personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;
- large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- using new technologies (for example surveillance systems).

You must take into account the nature, scope, context and purposes of the processing when deciding whether or not it is likely to result in a high risk to individuals' rights and freedoms.

How do we carry out a DPIA?

A DPIA must contain:

- at least a general description of your processing operations and the purposes;
- an assessment of the risks to the rights and freedoms of individuals;
- the measures envisaged to address those risks;
- the safeguards, security measures and mechanisms in place to ensure you protect the personal data; and
- a demonstration of how you are complying with Part 3 of the Act, taking into account the rights and legitimate interests of the data subjects and any other people concerned.

When do we need to send our DPIA to the ICO?

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

The Information Commissioner will respond within **six weeks**. This timescale may increase by a further month, depending on the complexity of the processing you intend to carry out.

For detail on how to submit a DPIA to the ICO, please see 'Do we need to consult the ICO?'.

Example

A police force is considering using a commercially available drone system for surveillance purposes. By conducting a DPIA prior to any purchase of the equipment or processing taking place, the force can establish whether or not the equipment offers adequate security for the recording, and if the use of the system is proportionate or poses a high risk to the rights and freedoms of any individuals.

If they discover high risks after conducting a DPIA, and cannot easily mitigate any residual risk, the police force should consider consulting with the Information Commissioner for further guidance or approval.

Further Reading

Relevant provisions of the Act - See Sections 64, 65, Chapter 4
External link

Data protection officers

At a glance

- Data protection officers (DPOs) assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

In brief

When do we need to appoint a data protection officer for Law Enforcement processing?

Under the Part 3 of the Act, you must appoint a data protection officer (DPO) unless you are a court, or other judicial authority acting in a judicial capacity.

You may appoint a single data protection officer to act for a group of controllers, taking into account their structure and size.

Regardless of whether the UK GDPR or Part 3 of the Act obliges you to appoint a DPO, you must ensure that relevant staff have sufficient skills and expertise to discharge your obligations.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Part 3, Chapter 4 of the Act:

- to inform and advise the controller, its employees, and any associated processors about their obligations to comply with the UK GDPR and other relevant data protection laws such as Part 3 of the Act;
- to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

What does the Part 3 of the Act say about employer duties?

You must ensure that:

- the DPO reports to the highest relevant management level of your organisation – ie board level;
- the DPO operates independently, and is not dismissed or penalised for performing their task, however a DPO can still be dismissed or penalised for misconduct or negligence relating to their task; and
- you provide adequate resources to enable DPOs to meet their obligations under UK GDPR or Part 3 of the Act.

Can we allocate the role of DPO to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.

You can also contract out the role of DPO externally.

Does the DPO need specific qualifications?

The UK GDPR or Part 3 of the Act does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.

Further Reading

> Relevant provisions of the Act - See Sections 69 to 71, Chapter 4
> External link

Personal data breaches

At a glance

- Part 3 of the DPA 2018 introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner. You must do this within **72 hours** of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place.

In brief

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

What breaches do we need to notify the ICO?

You only have to notify the ICO of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If left **unaddressed** such a breach is likely to have a significant detrimental effect on individuals. For example:

- result in discrimination;
- damage to reputation;
- financial loss; or
- loss of confidentiality or any other significant economic or social disadvantage.

In more serious cases, for example those involving victims and witnesses, a personal data breach may cause more significant detrimental effects on individuals.

You have to assess this on a case by case basis and you need to be able to justify your decision to report a

breach to the Information Commissioner.

What information must a breach notification to the Information Commissioner contain?

You must include:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned;
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if you have one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

When do we have to tell individuals about a breach?

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, you must inform those concerned directly without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

The duty to tell an individual about a breach does not apply if:

- you have implemented appropriate technical and organisational measures which were applied to the personal data affected by the breach (for example the data has been securely encrypted);
- you have taken subsequent measures which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialise; or
- it would involve disproportionate effort.

Where a communication of a breach would involve disproportionate effort, you must make the information available to individuals in another, equally effective way, such as a public communication.

You may restrict the information, either wholly or partly, that you provide to individuals affected by a breach under certain circumstances. This is when doing so is a necessary and proportionate measure:

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

What information should we tell individuals who have been affected by the breach?

You must give individuals information including:

- a description of the nature of the personal data breach;
- the name and contact details of the data protection officer (if relevant) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

How do we notify a breach?

You have to report a notifiable breach to the ICO without undue delay and within 72 hours of when you became aware of it. Part 3 of the DPA 2018 recognises that it will often be impossible for you to investigate a breach fully within that time-period and allows you to provide information in phases. If you cannot provide all the information required above within 72 hours, you must also explain reasons for the delay in your breach notification.

If the breach is sufficiently serious to warrant notification to the public, you must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to £8.7m or 2 per cent of your global turnover.

To notify the ICO of a personal data breach, please see our pages on reporting a breach.

What should we do to prepare for breach reporting?

You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will help decision-making about whether you need to notify the Information Commissioner or the affected individuals.

In light of the tight timescales for reporting a breach, it is important to have robust breach detection, containment, management and mitigation policies and procedures in place.

Further Reading

> Relevant provisions of the DPA 2018 - See Sections 67, 68, Chapter 4
> External link

National security provisions

At a glance

- Under Part 3 of the DPA 2018 individuals have rights of access, rectification, erasure or restriction, and to not be subject to automated decision-making.
- Some of these rights may be limited or restricted where this is a necessary and proportionate measure to protect national security. For ease of reference, these restrictions are referred to in this guidance as the national security provisions.
- The national security provisions may also limit your obligation to inform individuals about personal data breaches, where this is necessary and proportionate to protect national security.
- The national security provisions do not apply in a blanket manner. You must be able to show that deviating from specified data protection standards is necessary and proportionate to safeguard 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 relating to the national security provision you wish to apply. You may rely on the certificate as conclusive evidence that the provision is a necessary and proportionate measure to protect national security. You should not assume that you must apply the provision, simply because a certificate has been issued. We publish details of relevant certificates.
- There is no exemption from, or restriction to, the data protection principles. You must always ensure your processing is generally fair and lawful, and complies with the other data protection principles.
- You must always comply with your general accountability and governance obligations.

Checklist for using the national security provisions

☐ We are a competent authority processing for law enforcement purposes.

☐ Our processing is fair and lawful, and we comply with the data protection principles.

☐ We comply with the data protection rights and obligations wherever possible, unless a restriction or limitation is necessary and proportionate to protect national security.

☐ We have considered the rights and legitimate interests of the individual, and have concluded that applying the national security provisions are a necessary and proportionate measure in the circumstances.

☐ We can point to a link between giving full effect to individuals' rights, or fully complying with our personal data breach obligations, and a potential adverse effect on national security.

☐ We have considered whether a national security certificate is applicable in the circumstances.

☐ We do not apply the national security provisions in a blanket manner, but only to the extent required to protect national security.

☐ We have considered whether we can inform the individual of the use of the provision, or whether

this would itself undermine national security.

☐ We have recorded the use of the provision and can demonstrate its necessity and proportionality in light of the individual's rights and legitimate interests.

In brief

Does this guidance apply to us?

This guidance applies to you if you are a competent authority processing for law enforcement purposes related to national security.

The rules governing law enforcement processing are set out in Part 3 of the DPA 2018.

If you are a competent authority processing data for a non-law enforcement purpose (eg for national security purposes only), the UK GDPR will apply to this processing. You should refer to our Guide to the UK GDPR.

If you are not a competent authority, and are processing personal data under the UK GDPR, different provisions apply. You should read our Guide to the UK GDPR.

The intelligence services themselves (or processors acting on their behalf) are covered by a separate regime. For more information, see our Guide to Intelligence Services Processing.

Further reading – ICO guidance

About the DPA 2018

What are the national security provisions?

The rights that individuals have when their data is being processed for law enforcement purposes are set out in sections 44 to 49 of the DPA 2018.

Some of these rights may be limited or restricted in certain circumstances. These circumstances are laid out in the provisions which set out the right. One of these circumstances is when restricting the right is

necessary and proportionate to protect national security.

Section 68 sets out your obligations as a controller to inform individuals of a personal data breach which would be likely to result in a risk to their rights and freedoms. This obligation can be limited under certain circumstances. One of these circumstances is when limiting the information you provide is necessary and proportionate to protect national security.

For ease of reference, these restrictions and limitations are referred to in this guidance as the national security provisions.

You must still comply with the data protection principles, and with your accountability and governance obligations.

Further Reading

> Key provisions in the DPA 2018 - see sections 45; 46; 47; 48; 51; 68; 79
> External link

Further reading – ICO guidance

Principles
Accountability and governance

What does national security cover?

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.

What are the effects of the national security provisions?

The provisions may permit you to restrict some of the data protection rights of individuals. The effects vary depending on the different rights. But in each instance, you can only apply the provision where this is a necessary and proportionate measure to protect national security.

Under the right to be informed, individuals have the right to be given privacy information about the collection and use of their personal data. You may be able to withhold some of this information, where this is necessary and proportionate to protect national security. Specifically, you may be able to withhold information about:

- the legal basis for processing;
- the length of time data will be retained for;
- the categories of any recipients of data; and
- any other further information you may normally provide to enable individuals to exercise their right of access.

You should provide as much of this information as you can, and only restrict the information where necessary and proportionate to protect national security.

Under the right of access, you may be able to withhold confirmation that you are processing personal data about a particular individual, and refuse to provide access to the data. Again, you should provide access to as much of the data as you can, and only withhold data where necessary and proportionate to protect national security.

Under the rights to rectification, erasure and the restriction of processing you would normally have to inform an individual exercising these rights whether you had refused their rights. However, you may be able to avoid informing them of this, to the extent that this is a necessary and proportionate measure to protect national security.

When dealing with a personal data breach, you would normally have to notify individuals who may be affected, if the breach is likely to result in a high risk to their rights and freedoms. However, you may be able to withhold this notification, where necessary and proportionate to protect national security.

When are the national security provisions likely to apply?

You can rely on the national security provisions to restrict individuals' rights or limit your personal data breach obligations, if you can show that doing so is a necessary and proportionate measure to protect national security. This is linked to human rights standards, which mean that any interference with privacy rights must be necessary and proportionate in a democratic society to meet a pressing social need.

Although you are permitted to apply the national security provisions, where necessary and proportionate, you cannot do this in a blanket manner. Instead you need to consider applying the national security provisions on a case-by-case basis. In particular, it's not enough simply that the processing is related to national security. You must consider the actual consequences to national security if you had to provide the relevant information to the individual. If you can reasonably provide that information without affecting national security, you must do so (subject, of course, to any other restrictions that might apply in the specific circumstances).

When you consider whether to rely on a provision to withhold information, you must also consider whether you should withhold it "wholly or partly". In practice, this means that you must try and provide as much information to individuals as possible, and only withhold what is necessary to protect national security. So, if you can provide some information without posing any significant risk to national security, you must do so.

You don't need to show that providing the information 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 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.

So, before withholding information you must first consider the fundamental rights and legitimate interests of the individual, and how these may be affected.

You must then consider whether withholding the information is a necessary and proportionate measure to protect national security. Keep in mind that there may be circumstances where the adverse effect on an individual could outweigh any trivial, or hypothetical risk to national security.

You must disclose it if, having considered this, you conclude that withholding the information is not necessary or proportionate.

If you decide to apply a national security provision, you should be able to make a reasoned and convincing argument about why this was necessary and proportionate. We may ask you for these arguments if we have received a complaint. You may base these on hypothetical scenarios, as long as they are realistic and credible.

For example, you may need to limit your response to a request under the right of access. You may apply a national security provision in order to provide a consistent "neither confirm nor deny" (NCND) response about whether you process data for national security purposes. This may be necessary even in a case where there is no direct impact on national security, so that nothing can be inferred in other cases which might have more of an impact on national security.

You can apply this type of NCND response as a general policy. However, you should be able to make a reasoned argument about its use and demonstrate it to the ICO if required. 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.

The following example illustrates the process that a competent authority might go through to consider the application of the national security provisions. Although in practice you might consider the application of other restrictions first, this example shows how the process might work and how you may take NCND considerations into account.

Example

A police force receives a subject access request from an individual who is a subject of a covert counter-terrorism investigation. The police can apply a national security provision to restrict the individual's access to their personal data if this would risk harm to the investigation. For example by tipping off the individual about the investigation, or providing them with an opportunity to evade or frustrate the investigation.

Before applying the provision, the police need to consider whether the individual's rights or legitimate interests would be adversely affected. The individual's right of access would clearly be adversely affected. The police need to consider whether restricting the individual's right to access their personal data is a necessary and proportionate measure in light of the purpose for which they are restricting the rights, and the importance of the investigation in protecting national security.

The police do not have to inform the individual that their rights have been restricted, or the reasons for the restriction, if doing so would harm the investigation and pose a risk to national security. The police

still need to inform the individual in general terms of their right to complain to the ICO or to apply to a court.

Once the investigation is complete, the police do not have to revisit the original subject access request, but if they receive a new request, they have to consider whether the restriction is still necessary. For example, to protect confidential sources, or other associated investigations. They also need to consider whether the restriction could be fully or partially removed.

Further reading – ICO guidance

The courts have considered a very similar exemption in the context of freedom of information requests. For more information, see our guidance on the FOI exemption for safeguarding national security.

What should we do if we restrict individuals' rights?

If you have restricted an individual's rights, you should normally inform them about:

- the restriction and the reasons for the restriction;
- their right to ask the ICO to check the restriction is lawful; and
- their right to bring a complaint to the ICO or apply to a court.

However, you may not have to inform individuals about the restriction and the reasons for it, if providing this information would itself undermine the purpose of the restriction.

Instead, you may consider issuing a more non-committal response. However, you should still provide anything which does not undermine the restriction. Wherever possible, also provide them with some information about their rights, in general terms. So, if you have refused to comply with an individual's request, you must still tell them about their right to complain to the ICO, or to apply to a court.

Individuals have the right to ask the ICO to check that any such refusal or restriction was lawful. This does not mean that the individual is able to circumvent the restriction and exercise their rights through the ICO instead. In many cases, we may be unable to be very specific about our findings because that might in itself reveal information which would prejudice the purposes the exemptions are designed to protect.

You need to record the restriction, and your reasons for applying it, so that you can show the ICO your reasons, if requested. You need to be able to show that you have applied the restriction only as far as necessary. Remember that you can apply the restriction wholly or partly to the right, and you should avoid applying it wholly unless that is necessary for protecting national security.

What is a ministerial certificate?

Section 79 of the DPA says that certain Ministers of the Crown (specifically, a member of the Cabinet, the Attorney General or the Advocate General for Scotland) can sign a certificate which is conclusive evidence that the restriction is a necessary and proportionate measure to protect national security.

It is important to remember that a certificate is not required in order for you to rely on the national security

provisions. In fact in most cases, you will determine for yourself whether a restriction or limitation is required to safeguard national security (ie the application of a national security provision).

The provisions and the ministerial certificate do different things. The provisions, as detailed above, are always available and you may properly apply them to safeguard national security, with or without a ministerial certificate. Ministerial certificates are meant to give greater legal certainty that national security is applicable for specified data processing. This is because certificates certify that a restriction is a necessary and proportionate measure to protect national security.

In this context, a ministerial certificate is admissible as conclusive evidence that a restriction of an individual's rights or a limitation on a controller's obligations is necessary to protect national security.

These certificates can apply in advance, or they can be issued retrospectively for a restriction applied by a competent authority. The ICO publishes some details of all national security certificates which have been issued, including the text of the certificate where possible. However, there may be some cases where the text of the certificate is sensitive and cannot be published. In these cases, we publish the fact that a certificate was issued, the date it was signed, and which minister signed it.

If a relevant certificate is in place, you can rely on it to demonstrate that the restriction is necessary and proportionate. However, you should always consider whether you need to apply a restriction, or rely on any associated certificate, in a particular case. Individuals may challenge inappropriate reliance on a ministerial certificate in the Tribunal.

If you consider that a certificate is required, you can apply to a Minister of the Crown to issue a national security certificate under section 79. Details of the process for doing this are on the Home Office website, and linked to from the National Security Certificate page of the ICO website.

Individuals directly affected by a certificate can appeal against it to the Upper Tribunal. The certificate may be quashed if the Tribunal considers that the Minister did not have reasonable grounds for issuing it.

Individuals may also appeal to the Tribunal on the basis that the restriction the competent authority is relying on does not fall within the general description in the certificate.

For more information on ministerial certificates, see the Guide to Intelligence Services Processing.

Penalties

At a glance

- The Information Commissioner can issue a monetary penalty for failing to comply with Part 3 of the Act.
- There are two tiers of penalty – the higher maximum and the standard maximum.

In brief

What penalties can the Information Commissioner issue?

The Information Commissioner has the power to issue a monetary penalty for an infringement of the provisions of Part 3 of the Act – Law Enforcement Processing. Any penalty that we issue is intended to be effective, proportionate and dissuasive, and will be decided on a case by case basis.

Under Part 6 of the Act, there are two tiers of penalty for an infringement of Part 3 - the higher maximum and the standard maximum.

What is the higher maximum?

The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries.

What is the standard maximum?

If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

Further Reading

Relevant provisions of the Act - See Sections 155 to 159, Part 6
External link

International transfers

At a glance

- Part 3, Chapter 5 deals with when you can transfer personal data to a **third country**.
- A third country is a country or territory outside the UK.
- The DPA 2018 places limits on the circumstances when you can share.
- You have to meet certain conditions, including that the transfer is for one of the law enforcement purposes.
- Mostly, you can transfer to a **'relevant authority'** - a body entrusted with similar law enforcement responsibilities in the third country.
- There are specific provisions if you transfer to bodies that are not relevant authorities, with additional requirements which you must meet before you can do this.

Checklists

- ☐ We have checked whether we are a competent authority as defined by Schedule 7 of the DPA 2018.
- ☐ We have checked that the recipient is a relevant authority.
- ☐ We have confirmed whether the data was received from another competent authority.
- ☐ The transfer is necessary for one of the law enforcement purposes.
- ☐ The transfer is covered by adequacy regulations.
- ☐ If not, we are satisfied that the data will be subject to appropriate safeguards once transferred, and have notified the ICO about the categories of transfer we make on this basis.
- ☐ We are satisfied that the data will be subject to appropriate safeguards once transferred, and have notified the ICO about the categories of transfer we make on this basis.
- ☐ If not, we have identified special circumstances which still require the data to be transferred.
- ☐ We have taken steps to ensure that the data will not be further transferred elsewhere, and we have ensured that appropriate safeguards and conditions for any such onward transfer are in place, including limits on the extent of these transfers.
- ☐ If the transfer is to a recipient who is not a relevant authority, we have checked it meets the additional conditions, and we have notified the ICO.

☐ We have documented the transfer.

In brief

What are the general principles for the transfer of personal data?

There are three conditions that you have to meet before you can make a transfer:

- The transfer has to be necessary for any of the law enforcement purposes.
- The transfer has to be based on either a finding of adequacy in respect of the third country, or where other appropriate safeguards are in place, or if not, that the transfer is for certain specified special circumstances.
- The transfer is to a relevant authority in the third country, or is a 'relevant international organisation' ie an international body that carries out functions for any of the law enforcement purposes.

However it is still possible to transfer personal data to a body which is not a relevant authority, if you meet certain additional safeguards. See Can we make a transfer to recipients other than relevant authorities?

If the data is obtained from a competent authority in another EU member State, then that competent authority has to authorise the transfer. Except if:

- there is an immediate and serious threat to the public security of a third country; or
- there is an immediate and serious threat to the essential interests of an EU member State; and
- authorisation cannot be obtained in good time.

In such cases you must inform the relevant competent authority which would have been responsible for authorising the transfer without delay.

Is the transfer covered by an adequacy decision?

You may transfer personal data if the transfer is covered by UK adequacy regulations.

Adequacy regulations confirm that a particular third country (or a specified territory or sector in a third country) or international organisation has an adequate data protection regime to protect personal data. This is sometimes referred to as an 'adequacy decision'.

As at October 2019, there are adequacy regulations in place to cover transfers to:

- EEA States. (The EU member states and Iceland, Liechtenstein and Norway); and

- Switzerland; and
- Gibraltar.

Can we make a transfer subject to appropriate safeguards?

If there is no 'adequacy decision' about the country, territory or sector for your restricted transfer, you may still make the transfer on the basis that other appropriate safeguards exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.

Appropriate safeguards may be provided for by:

- a legal instrument providing appropriate safeguards which binds the intended recipient; or
- an assessment performed by the controller which concludes that appropriate safeguards exist. In this case, you must inform the Information Commissioner of the categories of data transfers that take place.

You must document the transfer, and provide this documentation to the Information Commissioner on request. You must record:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;
- the justification for the transfer; and
- a description of the data you transferred.

You must ensure that any personal data you have transferred is not further transferred to another third country without your authorisation, or authorisation from another UK competent authority, and any authorisation can only be given where the transfer is necessary for any of the law enforcement purposes.

Are there any special circumstances?

Sometimes, you may need to transfer personal data when there is neither a finding of adequacy, nor appropriate safeguards in place. This can only take place in certain, specified circumstances, referred to as the 'special circumstances'. These are listed in the DPA 2018 as the five circumstances where the transfer is necessary:

> 1. To protect the vital interests of the data subject or another person;
> 2. To safeguard the legitimate interests of the data subject;
> 3. For the prevention of an immediate and serious threat to the public security of third country;
> 4. In individual cases for any of the law enforcement purposes; or
> 5. In individual cases for a legal purpose.

There are a few things to keep in mind.

You need to document the transfer, and provide those records to the Information Commissioner on request. You must record:

- the date and time of the transfer;
- the name, and any other pertinent information about the recipient;
- the justification for the transfer; and
- a description of the personal data you transferred.

These are the same details that you are required to record for transfers on the basis of appropriate safeguards.

Items 4 and 5 of the special circumstances provide for a degree of flexibility, but in those cases it is necessary for you to specifically consider the rights and freedoms of the individual whose data you are transferring. If those rights and freedoms override any public interest in the transfer, then the transfer cannot take place on the basis of special circumstances. Items 4 and 5 are case-specific and this safeguard is there to make sure that the individual's interests remain at the heart of matters. In such cases, if the transfer is still necessary, you will need to apply another lawful basis for the transfer.

A transfer is deemed to be necessary under item 5:

- for the purpose of, or in connection with, any legal proceedings for any of the law enforcement purposes. This can include prospective legal proceedings, ie where the proceedings are anticipated, but have not yet commenced;
- for the purpose of obtaining legal advice in relation to any of the law enforcement purposes; or
- for the purpose of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.

In each case, the circumstances must link directly back to any of the law enforcement purposes to which Part 3 of the Act relates.

Can we make a transfer to recipients other than relevant authorities?

For the most part, it is expected that transfers will take place between 'relevant authorities', or relevant international organisations ie to any (legal) person in the third country (or operating internationally) who has functions comparable to those of a 'competent authority' for the purposes of Part 3 of the DPA 2018.

Sometimes, however, you may need to transfer personal data to a recipient that is not a relevant authority. Before you can do this, you must meet all four of these additional conditions:

1. The transfer is strictly necessary in a specific case, for the performance of a task by the transferring controller, as provided by law for any of the law enforcement purposes.

In item 1, the term 'strictly necessary' implies a condition more demanding that merely 'necessary'. The term 'strictly necessary' should be interpreted to make any consideration of the necessity rather more stringent in the specific circumstances.

Further, the transfer must be for the performance of a task for which you have a lawful purpose under the law enforcement provisions of Part 3 of the DPA 2018.

2. The fundamental rights and freedoms of the data subject do not override the public interest concerning the transfer.

Item 2 means that the rights and freedoms of the data subject can override any public interest in the transfer, so if the rights and freedoms of the data subject in not having their data transferred to the intended recipient are of equal or greater importance than the public interest in transferring the data, then the transfer shall not take place.

3. The transferring controller considers that the transfer to a relevant authority in the third country would be ineffective, or inappropriate.

Item 3 means that, where possible, transfers to a third country should be undertaken to a relevant authority in that country, and it is only in circumstances where transferring the data to such a relevant authority would be ineffective or inappropriate, that a transfer to another recipient should be contemplated. Transfers may be ineffective, for example, if the transfer is time-critical and the relevant authority would be unable to act on the transfer in sufficient time. A transfer may be inappropriate if the transfer to the relevant authority might prejudice the purposes of the transfer, for example if the data relate to allegations of corruption or impropriety in the relevant authority and there is a risk that the transfer may tip-off relevant personnel within that authority that an investigation is underway.

Where you have transferred data to a body other than a relevant authority, you must inform the relevant authority in that country of the transfer, unless, as above, that would be ineffective or inappropriate.

4. The transferring controller sets out the specific purposes for which the data may be processed by the intended recipient and informs them of these.

You need to document the transfer, and you also need to notify the Information Commissioner about the transfer. This is different to other types of transfers, where you record the details but only have to provide them to the Commissioner on request.

What happens to subsequent transfers?

It is important that control of personal data is not lost once you have transferred it. It is vital that the rights and freedoms of individuals are still uppermost. Therefore, if the data you transferred is to be subsequently transferred elsewhere, it is important that those rights and freedoms continue to follow the data. For this reason, there are certain provisions that you must observe before any subsequent transfer can take place.

Firstly, you must make it a condition of the transfer that any subsequent transfer must be authorised by you, or another competent authority. It would be sensible to have agreements in place with any other competent authorities who you may consider allowing to make such an authorisation.

Secondly, any authorisation can only be for a transfer which is necessary for any of the law enforcement purposes, and you must give consideration to:

- the seriousness of the circumstances leading to the request for authorisation of the subsequent transfer;
- the purpose for which you originally transferred the data; and
- the standards of data protection which apply in the country or international organisation where the data will be transferred.

If you originally received the data from a competent authority in an EU member state, that competent authority must first authorise the transfer before you in turn can authorise it. This creates a chain of accountability, linking back to the original competent authority which first held the data, which ensures that the original competent authority retains a measure of control and influence over any processing of that data.

The only exception is if the transfer is necessary for the prevention of an immediate and serious threat to the public security of a third country, or to the essential interests of an EU member state (note, not the essential interests of any third country) and you cannot obtain authorisation from the originating competent authority in good time. If that happens, then you should inform the originating competent authority without delay.

Further Reading

Relevant provisions of the legislation - see DPA 2018 sections 72 to 78, Chapter 5
External link

Resources

This page contains resources and support that organisations in the police, justice and surveillance sector may find useful.

Appropriate policy document

Further Reading

Part 3 - appropriate policy document
For organisations
Word (71.09K)

Paying the data protection fee

On 1 April 2019, the rules around paying the data protection fee changed. Members of the House of Lords, elected representatives and prospective representatives **(including police and crime commissioners)** are exempt from paying a fee, unless they process personal data for purposes other than the exercise of their functions as a Member of the House of Lords, an elected representative or as a prospective representative. For more information, read our guidance on the data protection fee.

The use of live facial recognition technology by law enforcement in public places

The Information Commissioner has issued the first Commissioner's Opinion under data protection law about the use of live facial recognition technology be law enforcement.

Further Reading

Commissioner's opinion
External link

Processing gangs information: a checklist for police forces

The ICO recently issued an Enforcement Notice to the Metropolitan Police Service (MPS) in relation to their Gangs Matrix, after we found it breached data protection laws. You can read a blog about it. The ICO is also investigating how information about gangs is used by other public authorities.

This checklist has been created specifically for police forces who might be using, or considering using, a Gangs Matrix, or similar system. Please note that the checklist will help you to assess compliance with data protection law, and is a guide – not a guarantee of compliance.

Surveillance

Our team often receives enquiries about surveillance technology including body worn video, ANPR and unmanned aerial systems. Advice about these technologies is provided in the updated version of the CCTV code of practice. The code sets out the Information Commissioner's recommendations on how organisations can process personal data within the legal requirements of the Data Protection Act when using these technologies.

Toolkit for organisations considering using data analytics

A toolkit designed to help the law enforcement sector comply with data protection law when using data analytics has been created by the ICO. The toolkit will be most helpful to you if your organisation is at the beginning of your data analytics project lifecycle. It will help you to recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics.

Further Reading

CCTV code of practice
For organisations
File (0 bytes)

The Home Office has published detailed guidance for police forces about the use of body worn video (BWV), which takes into account the management of personal data obtained by the cameras.

Further reading

Home Office guidance - Safeguarding body worn video data
External link

Home Office guidance - Technical guidance for body worn video devices
External link

Guidance about data protection concerns and BWV was also produced by The College of Policing in August 2014.

Further Reading

College of Policing guidance - Body Worn Video
External link

You may also be interested in reading our guide on the responsible recreational use of drones – also called unmanned aerial systems (UAS) or unmanned aerial vehicles (UAVs).

We liaise with the Surveillance Camera Commissioner where appropriate. The Surveillance Camera Commissioner has also produced a code of practice.

Further Reading

Surveillance camera code of practice
External link

There is more information available about the role of the Surveillance Camera Commissioner and the tools available to help with compliance.

Further Reading

Surveillance Camera Commissioner
External link

Security

Data Controllers must ensure that they take appropriate technical and organisational measures against unlawful or unauthorised processing, accidental loss, destruction or damage to personal data. Some of the ICO's largest civil monetary penalties have been served on data controllers in the police, justice and borders sectors. This frequently occurs where insufficient safeguards have been in place for handling sensitive personal data. Here you will find advice on security measures safeguarding cloud computing and privacy impact assessments.

Further Reading

Cloud computing guidance for organisations
For organisations
PDF (497.37K)

Further reading

Further reading

City of London Police follow up
Action we've taken

Independent Office for Police Conduct follow up audit
Action we've taken

Humberside Police audit
Action we've taken