

Key definitions

Who does the UK GDPR apply to?

- The UK GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the UK GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the UK GDPR places further obligations on you to ensure your contracts with processors comply with the UK GDPR.
- The UK GDPR applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK.
- The UK GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 3, 28-31 and Recitals 22-25, 81-82 
External link

Controllers and processors

At a glance

- Understanding your role in relation to the personal data you are processing is crucial in ensuring compliance with the UK GDPR and the fair treatment of individuals.
- Your obligations under the UK GDPR will vary depending on whether you are a controller, joint controller or processor.
- The ICO has the power to take action against controllers and processors under the UK GDPR.
- Individuals can bring claims for compensation and damages against both controllers and processors.
- You should take the time to assess, and document, the status of each organisation you work with in respect of all the personal data and processing activities you carry out.
- Whether you are a controller or processor depends on a number of issues. The key question is – who determines the purposes for which the data are processed and the means of processing?
- Organisations that determine the purposes and means of processing will be controllers regardless of how they are described in any contract about processing services.

Checklists

The following checklists set out indicators as to whether you are a controller, a processor or a joint controller. The more boxes you tick, the more likely you are to fall within the relevant category.

Are we a controller?

- We decided to collect or process the personal data.
- We decided what the purpose or outcome of the processing was to be.
- We decided what personal data should be collected.
- We decided which individuals to collect personal data about.
- We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.
- We are processing the personal data as a result of a contract between us and the data subject.
- The data subjects are our employees.
- We make decisions about the individuals concerned as part of or as a result of the processing.
- We exercise professional judgement in the processing of the personal data.
- We have a direct relationship with the data subjects.

- We have complete autonomy as to how the personal data is processed.
- We have appointed the processors to process the personal data on our behalf.

Are we a joint controller?

- We have a common objective with others regarding the processing.
- We are processing the personal data for the same purpose as another controller.
- We are using the same set of personal data (eg one database) for this processing as another controller.
- We have designed this process with another controller.
- We have common information management rules with another controller.

Are we a processor?

- We are following instructions from someone else regarding the processing of personal data.
- We were given the personal data by a customer or similar third party, or told what data to collect.
- We do not decide to collect personal data from individuals.
- We do not decide what personal data should be collected from individuals.
- We do not decide the lawful basis for the use of that data.
- We do not decide what purpose or purposes the data will be used for.
- We do not decide whether to disclose the data, or to whom.
- We do not decide how long to retain the data.
- We may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- We are not interested in the end result of the processing.

In brief

- What are 'controllers' and 'processors'?
- How do you determine whether you are a controller or processor?
- What does it mean if you are a controller?
- What does it mean if you are a processor?
- What does it mean if you are joint controllers?
- In more detail

What are 'controllers' and 'processors'?

Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Processors act on behalf of, and only on the instructions of, the relevant controller.

How do you determine whether you are a controller or processor?

You should be able to differentiate between controllers, joint controllers and processors so you understand which UK GDPR obligations apply to which organisation.

To determine whether you are a controller or processor, you will need to consider your role and responsibilities in relation to your data processing activities.

If you exercise overall control of the purpose and means of the processing of personal data – ie, you decide what data to process and why – you are a controller.

If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data.

What does it mean if you are a controller?

Controllers shoulder the highest level of compliance responsibility – you must comply with, and demonstrate compliance with, all the data protection principles as well as the other UK GDPR requirements. You are also responsible for the compliance of your processor(s).

The Information Commissioner's Office (ICO) and individuals may take action against a controller regarding a breach of its obligations.

Controllers in the UK must pay the data protection fee, unless they are exempt.

What does it mean if you are a processor?

Processors do not have the same obligations as controllers under the UK GDPR and do not have to pay a data protection fee. However, if you are a processor, you do have a number of direct obligations of your

own under the UK GDPR.

Both the ICO and individuals may take action against a processor regarding a breach of those obligations.

What does it mean if you are joint controllers?

Joint controllers must arrange between themselves who will take primary responsibility for complying with UK GDPR obligations, and in particular transparency obligations and individuals' rights. They should make this information available to individuals.

However, all joint controllers remain responsible for compliance with the controller obligations under the UK GDPR. Both the ICO and individuals may take action against any controller regarding a breach of those obligations.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 4(7), 4(8), 5(1), 5(2), 26, 28 – 36 and Recitals 28, 79, 81 – 83 

External link

Further reading – ICO guidance

[Contracts and liabilities between controllers and processors](#)

In more detail – ICO guidance

We have produced [more detailed guidance on controllers and processors](#)

What is personal data?

At a glance

- Understanding whether you are processing personal data is critical to understanding whether the UK GDPR applies to your activities.
- Personal data is information that relates to an identified or identifiable individual.
- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.
- When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.
- It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.
- Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of UK GDPR.
- Information which is truly anonymous is not covered by the UK GDPR.
- If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

In brief

- [What is personal data?](#)
- [What are identifiers and related factors?](#)
- [Can we identify an individual directly from the information we have?](#)
- [Can we identify an individual indirectly from the information we have \(together with other available information\)?](#)
- [What is the meaning of 'relates to'?](#)
- [What happens when different organisations process the same data for different purposes?](#)
- [In more detail](#)

What is personal data?

- The UK GDPR applies to the processing of personal data that is:
 - wholly or partly by automated means; or
 - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
 - can be identified or who are identifiable, directly from the information in question; or
 - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The UK GDPR provides a non-exhaustive list of identifiers, including:
 - name;
 - identification number;
 - location data; and
 - an online identifier.
- 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.

Can we identify an individual directly from the information we have?

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.

- If an individual is directly identifiable from the information, this may constitute personal data.

Can we identify an individual indirectly from the information we have (together with other available information)?

- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

What is the meaning of ‘relates to’?

- Information must ‘relate to’ the identifiable individual to be personal data.
- This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether or not data relates to an individual, you may need to consider:
 - the content of the data – is it directly about the individual or their activities?;
 - the purpose you will process the data for; and
 - the results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.
- Inaccurate information may still be personal data if it relates to an identifiable individual.

What happens when different organisations process the same data for different purposes?

- It is possible that although data does not relate to an identifiable individual for one controller, in the hands of another controller it does.
- This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant and the data therefore does not relate to them.
- However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.

- It is therefore necessary to consider carefully the purpose for which the controller is using the data in order to decide whether it relates to an individual.
- You should take care when you make an analysis of this nature.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51 

External link

In more detail – ICO guidance

We have published detailed guidance on [determining what is personal data](#).

Principles

At a glance

- The UK GDPR sets out seven key principles:
 - Lawfulness, fairness and transparency
 - Purpose limitation
 - Data minimisation
 - Accuracy
 - Storage limitation
 - Integrity and confidentiality (security)
 - Accountability
- These principles should lie at the heart of your approach to processing personal data.

In brief

- [What are the principles?](#)
- [Why are the principles important?](#)

What are the principles?

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

“

- “(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- “(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- “(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- “(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

“

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

For more detail on each principle, please read the relevant page of this guide.

Why are the principles important?

The principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection 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 the UK GDPR.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

Further Reading

 Relevant provisions in the UK GDPR - See Article 5 and Recital 39, and Chapter III (rights), Chapter V (international transfers) and Article 82 (fines) 
External link

In more detail – ICO guidance

Read our [individual rights](#) and [international transfers](#) guidance.

Accountability principle

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance.

For more information, see the [accountability and governance](#) section of this guide.

Integrity and confidentiality (security)

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

For more information, see the [security](#) section of this guide.

Storage limitation

At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Checklist

- We know what personal data we hold and why we need it.
- We carefully consider and can justify how long we keep personal data.
- We have a policy with standard retention periods where possible, in line with documentation obligations.
- We regularly review our information and erase or anonymise personal data when we no longer need it.
- We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
- We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Other resources

For more detailed checklists and practice advice on retention, please use the ICO's [self-assessment toolkit - records management checklist](#)

In brief

- What is the storage limitation principle?
- Why is storage limitation important?
- Do we need a retention policy?
- How should we set retention periods?
- When should we review our retention?
- What should we do with personal data that we no longer need?
- How long can we keep personal data for archiving, research or statistical purposes?
- How does this apply to data sharing?

What is the storage limitation principle?

Article 5(1)(e) says:

“

"1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

So, even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it.

There are close links here with the data minimisation and accuracy principles.

The UK GDPR does not set specific time limits for different types of data. This is up to you, and will depend on how long you need the data for your specified purposes.

Why is storage limitation important?

Ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than you need, and there

may be unnecessary costs associated with storage and security.

Remember that you must also respond to subject access requests for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

Do we need a retention policy?

Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. They help you establish and document standard retention periods for different categories of personal data.

A retention schedule may form part of a broader 'information asset register' (IAR), or your general processing documentation.

To comply with [documentation requirements](#), you need to establish and document standard retention periods for different categories of information you hold wherever possible. It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate. For example, if you are not actually using a record, you should reconsider whether you need to retain it.

If you are a small organisation undertaking occasional low-risk processing, you may not need a documented retention policy.

However, if you don't have a retention policy (or if it doesn't cover all of the personal data you hold), you must still regularly review the data you hold, and delete or anonymise anything you no longer need.

Further reading – records management and retention schedules

[The National Archives \(TNA\)](#) publishes practical guidance for public authorities on a range of records management topics, including retention and disposal. This guidance can help you comply with the storage limitation principle (even if you are not a public authority):

[Disposing of records](#)

[FOI Records Management Code – Guide 8: Disposal of records](#)

[The Keeper of the Records of Scotland](#) also publishes guidance on Scottish public authorities' records management obligations, including [specific guidance on retention schedules](#).

How should we set retention periods?

The UK GDPR does not dictate how long you should keep personal data. It is up to you to justify this, based on your purposes for processing. You are in the best position to judge how long you need it.

You must also be able to justify why you need to keep personal data in a form that permits identification of

individuals. If you do not need to identify individuals, you should anonymise the data so that identification is no longer possible.

For example:

- You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies, but you should not keep data indefinitely 'just in case', or if there is only a small possibility that you will use it.

Example

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons for a further set time.

Example

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

Example

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – the agency should remove it from their systems unless there are good reasons for keeping it. For example, if the agency has also been asked to collect the debt on behalf of the creditor.

- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.

Example

A business may need to keep some personal data about a previous customer so that they can deal with any complaints the customer might make about the services they provided.

Example

An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details.

Example

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for direct marketing. It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If you keep personal data to comply with a requirement like this, you will not be considered to have kept the information for longer

than necessary.

- You should consider any relevant industry standards or guidelines. For example, credit reference agencies keep consumer credit data for six years. Industry guidelines are a good starting point for standard retention periods and are likely to take a considered approach. However, they do not guarantee compliance. You must still be able to explain why those periods are justified, and keep them under review.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and lawful.

When should we review our retention?

You should review whether you still need personal data at the end of any standard retention period, and erase or anonymise it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful if you hold many records of the same type.

It is also good practice to review your retention of personal data at regular intervals before this, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

If you don't have a set retention period for the personal data, you must regularly review whether you still need it.

However, there is no firm rule about how regular these reviews must be. Your resources may be a relevant factor here, along with the privacy risk to individuals. The important thing to remember is that you must be able to justify your retention and how often you review it.

You must also review whether you still need personal data if the individual asks you to. Individuals have the absolute right to erasure of personal data that you no longer need for your specified purposes.

What should we do with personal data that we no longer need?

You can either erase (delete) it, or anonymise it.

You need to remember that there is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still processing personal data. You should only store it offline (rather than delete it) if you can still justify holding it. You must be prepared to respond to subject access requests for personal data stored offline, and you must still comply with all the other principles and rights.

The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information on that system.

Further reading

We produced detailed guidance on the issues surrounding deletion under the 1998 Act. This will be updated for the UK GDPR in due course, but in the meantime still offers useful guidance on the

practical issues surrounding deletion:

[Deleting personal data](#)

Alternatively, you can anonymise the data so that it is no longer "in a form which permits identification of data subjects".

Personal data that has been pseudonymised – eg key-coded – will usually still permit identification. Pseudonymisation can be a useful tool for compliance with other principles such as data minimisation and security, but the storage limitation principle still applies.

How long can we keep personal data for archiving, research or statistical purposes?

You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes.

Although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. For example, pseudonymisation may be appropriate in some cases.

This must be your only purpose. If you justify indefinite retention on this basis, you cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. This does not prevent other organisations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the principles.

How does this apply to data sharing?

If you share personal data with other organisations, you should agree between you what happens once you no longer need to share the data. In some cases, it may be best to return the shared data to the organisation that supplied it without keeping a copy. In other cases, all of the organisations involved should delete their copies of the personal data.

Example

Personal data about the customers of Company A is shared with Company B, which is negotiating to buy Company A's business. The companies arrange for Company B to keep the information confidential, and use it only in connection with the proposed transaction. The sale does not go ahead and Company B returns the customer information to Company A without keeping a copy.

The organisations involved in an information-sharing initiative may each need to set their own retention periods, because some may have good reasons to retain personal data for longer than others. However, if you all only hold the data for the purposes of the data-sharing initiative and it is no longer needed for that initiative, then all organisations with copies of the information should delete it.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 5\(1\)\(e\), 17\(1\)\(a\), 30\(1\)\(f\) and 89, and Recital 39](#) 
External link

Further reading – ICO guidance

Read our guidance on [documentation](#) and the [right to erasure](#)

Accuracy

At a glance

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

Checklist

- We ensure the accuracy of any personal data we create.
- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

In brief

- [What is the accuracy principle?](#)
- [When is personal data 'accurate' or 'inaccurate'?](#)
- [What about records of mistakes?](#)
- [What about accuracy of opinions?](#)
- [Does personal data always have to be up to date?](#)
- [What steps do we need to take to ensure accuracy?](#)

- What should we do if an individual challenges the accuracy of their personal data?

What is the accuracy principle?

Article 5(1)(d) of the UK GDPR says:

“

“1. Personal data shall be:

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

This is the second of three principles about data standards, along with data minimisation and storage limitation.

There are clear links here to the [right to rectification](#), which gives individuals the right to have inaccurate personal data corrected.

In practice, this means that you must:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source and status of personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

When is personal data ‘accurate’ or ‘inaccurate’?

The UK GDPR does not define the word ‘accurate’. However, the Data Protection Act 2018 does say that ‘inaccurate’ means “incorrect or misleading as to any matter of fact”. It will usually be obvious whether personal data is accurate.

You must always be clear about what you intend the record of the personal data to show. What you use it for may affect whether it is accurate or not. For example, just because personal data has changed doesn’t mean that a historical record is inaccurate – but you must be clear that it is a historical record.

Example

If an individual moves house from London to Manchester a record saying that they currently live in London will obviously be inaccurate. However a record saying that the individual once lived in London remains accurate, even though they no longer live there.

Example

The Postcode Address File (PAF) contains UK property postal addresses. It is structured to reflect the way the Royal Mail delivers post. So it is common for someone to have a postal address linked to a town in one county (eg Stoke-on-Trent in Staffordshire) even if they actually live in another county (eg Cheshire) and pay council tax to that council. The PAF file is not intended to accurately reflect county boundaries.

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded.

However, you may legitimately need your records to accurately reflect the order of events – in this example, that a charge was imposed, but later cancelled or refunded. Keeping a record of the mistake and its correction might also be in the individual's best interests.

Example

A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.

It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

Example

An individual finds that, because of an error, their account with their existing energy supplier has been closed and an account opened with a new supplier. Understandably aggrieved, they believe the original account should be reinstated and no record kept of the unauthorised transfer. Although this reaction is understandable, if their existing supplier did close their account, and another supplier opened a new account, then records reflecting what actually happened will be accurate. In such cases it makes sense to ensure that the record clearly shows that an error occurred.

Example

An individual is dismissed for alleged misconduct. An Employment Tribunal finds that the dismissal was unfair and the individual is reinstated. The individual demands that the employer deletes all references to misconduct. However, the record of the dismissal is accurate. The Tribunal's decision was that the employee should not have been dismissed on those grounds. The employer should ensure its records reflect this.

What about accuracy of opinions?

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

Example

An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (which is an informed opinion) may prove to be incorrect after more extensive examination or further tests. However, if the patient's records reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect that doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later, and in data protection terms is required in order to comply with the 'adequacy' element of the data minimisation principle.

If an individual challenges the accuracy of an opinion, it is good practice to add a note recording the challenge and the reasons behind it.

How much weight is actually placed on an opinion is likely to depend on the experience and reliability of the

person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. However, this is not really an issue of accuracy. Instead, you need to consider whether the personal data is "adequate" for your purposes, in line with the data minimisation principle.

Note that some records that may appear to be opinions do not contain an opinion at all. For example, many financial institutions use credit scores to help them decide whether to provide credit. A credit score is a number that summarises the historical credit information on a credit report and provides a numerical predictor of the risk involved in granting an individual credit. Credit scores are based on a statistical analysis of individuals' personal data, rather than on a subjective opinion about their creditworthiness. However, you must ensure the accuracy (and adequacy) of the underlying data.

Does personal data always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers' changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information.

Example

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

You do not need to update personal data if this would defeat the purpose of the processing. For example, if you hold personal data only for statistical, historical or other research reasons, updating the data might defeat that purpose.

In some cases it is reasonable to rely on the individual to tell you when their personal data has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this.

Example

An organisation keeps addresses and contact details of previous customers for marketing purposes. It does not have to use data matching or tracing services to ensure its records are up to date – and it may actually be difficult to show that the processing involved in data matching or tracing for these purposes is fair, lawful and transparent.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message 'not at this address' marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should update its records to indicate that the address is no longer current.

What steps do we need to take to ensure accuracy?

Where you use your own resources to compile personal data about an individual, then you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. If, for example, you give an employee a pay increase on the basis of an annual increment and a performance bonus, then there is no excuse for getting the new salary figure wrong in your payroll records.

We recognise that it may be impractical to check the accuracy of personal data someone else provides. In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

What is a 'reasonable step' will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate. For example, employers may need to check the precise details of job applicants' education, qualifications and work experience if it is essential for that particular role, when they would need to obtain authoritative verification.

Example

An organisation recruiting a driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in his work history that he worked

as a Father Christmas in a department store 20 years ago does not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it is usually reasonable to assume that they have given you accurate information. However, in some circumstances you need to double-check – for example if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.

Example

A business that is closing down recommends a member of staff to another organisation. Assuming the two employers know each other, it may be reasonable for the organisation to which the recommendation is made to accept assurances about the individual's work experience at face value. However, if a particular skill or qualification is needed for the new job role, the organisation needs to make appropriate checks.

Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible.

What should we do if an individual challenges the accuracy of their personal data?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it.

Remember that individuals have the absolute right to have incorrect personal data rectified – see the [right to rectification](#) for more information.

Individuals don't have the right to erasure just because data is inaccurate. However, the accuracy principle requires you to take all reasonable steps to erase or rectify inaccurate data without delay, and it may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data it is therefore good practice to consider this request.

Further reading

↗ Relevant provisions in the UK GDPR - See Article 5(1)(d) and Article 16 (the right to rectification) and Article 17 (the right to erasure) ↗

External link

Further reading

Read our guidance on:

[The right to rectification](#)

[The right to erasure](#)

Data minimisation

At a glance

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Checklist

- We only collect personal data we actually need for our specified purposes.
- We have sufficient personal data to properly fulfil those purposes.
- We periodically review the data we hold, and delete anything we don't need.

In brief

- [What is the data minimisation principle?](#)
- [How do we decide what is adequate, relevant and limited?](#)
- [When could we be processing too much personal data?](#)
- [When could we be processing inadequate personal data?](#)
- [What about the adequacy and relevance of opinions?](#)

What is the data minimisation principle?

Article 5(1)(c) says:

“

“1. Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)”

So you should identify the minimum amount of personal data you need to fulfil your purpose. You should hold that much information, but no more.

This is the first of three principles about data standards, along with accuracy and storage limitation.

The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that the UK GDPR says individuals have the right to complete any incomplete data which is inadequate for your purpose, under the right to rectification. They also have right to get you to delete any data that is not necessary for your purpose, under the right to erasure (right to be forgotten).

How do we decide what is adequate, relevant and limited?

The UK GDPR does not define these terms. Clearly, though, this will depend on your specified purpose for collecting and using the personal data. It may also differ from one individual to another.

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it.

For special category data or criminal offence data, it is particularly important to make sure you collect and retain only the minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should in particular consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need. This is closely linked with the storage limitation principle.

When could we be processing too much personal data?

You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details.

Example

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

If you need to process particular information about certain individuals only, you should collect it just for

those individuals – the information is likely to be excessive and irrelevant in relation to other people.

Example

A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.

Example

An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.

If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach of the data minimisation principle. Individuals will also have the right to erasure.

When could we be processing inadequate personal data?

If the processing you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should not process personal data if it is insufficient for its intended purpose.

In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.

Example

A group of individuals set up a club. At the outset the club has only a handful of members, who all know each other, and the club's activities are administered using only basic information about the members' names and email addresses. The club proves to be very popular and its membership grows

rapidly. It becomes necessary to collect additional information about members so that the club can identify them properly, and so that it can keep track of their membership status, subscription payments etc.

Data may also be inadequate if you are making decisions about someone based on an incomplete understanding of the facts. In particular, if an individual asks you to supplement incomplete data under their right to rectification, this could indicate that the data might be inadequate for your purpose.

Obviously it makes no business sense to have inadequate personal data – but you must be careful not to go too far the other way and collect more than you need.

What about the adequacy and relevance of opinions?

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, you should make this clear.

Example

A GP's record may hold only a letter from a consultant and it will be the hospital file that contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable detailed records to be traced.

For more information about the accuracy of opinions, see our guidance on the accuracy principle.

Further Reading

 Relevant provisions in the UK GDPR - See Article 5(1)(c) and Recital 39, and Article 16 (right to rectification) and Article 17 (right to erasure) 

External link

Further reading

Read our guidance on:

[The storage limitation principle](#)

Purpose limitation

At a glance

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

Checklist

- We have clearly identified our purpose or purposes for processing.
- We have documented those purposes.
- We include details of our purposes in our privacy information for individuals.
- We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

In brief

- [What is the purpose limitation principle?](#)
- [Why do we need to specify our purposes?](#)
- [How do we specify our purposes?](#)
- [Once we collect data for a specified purpose, can we use it for other purposes?](#)
- [What is a 'compatible' purpose?](#)

What is the purpose limitation principle?

Article 5(1)(b) says:

“

"1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."

In practice, this means that you must:

- be clear from the outset why you are collecting personal data and what you intend to do with it;
- comply with your documentation obligations to specify your purposes;
- comply with your transparency obligations to inform individuals about your purposes; and
- ensure that if you plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

Why do we need to specify our purposes?

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid 'function creep'. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public trust in how you use personal data.

There are clear links with other principles – in particular, the fairness, lawfulness and transparency principle. Being clear about why you are processing personal data will help you to ensure your processing is fair, lawful and transparent. And if you use data for unfair, unlawful or 'invisible' reasons, it's likely to be a breach of both principles.

Specifying your purposes is necessary to comply with your accountability obligations.

How do we specify our purposes?

If you comply with your documentation and transparency obligations, you are likely to comply with the requirement to specify your purposes without doing anything more:

- You need to specify your purpose or purposes for processing personal data within the documentation you are required to keep as part of your records of processing (documentation) obligations under Article 30.
- You also need to specify your purposes in your privacy information for individuals.

However, you should also remember that whatever you document, and whatever you tell people, this cannot make fundamentally unfair processing fair and lawful.

If you are a small organisation and you are exempt from some documentation requirements, you may not need to formally document all of your purposes to comply with the purpose limitation principle. Listing your purposes in the privacy information you provide to individuals will be enough. However, it is still good practice to document all of your purposes. For more information, read our [documentation guidance](#).

If you have not provided privacy information because you are only using personal data for an obvious purpose that individuals already know about, the “specified purpose” should be taken to be the obvious purpose.

You should regularly review your processing, documentation and privacy information to check that your purposes have not evolved over time beyond those you originally specified ('function creep').

Once we collect personal data for a specified purpose, can we use it for other purposes?

The UK GDPR does not ban this altogether, but there are restrictions. In essence, if your purposes change over time or you want to use data for a new purpose which you did not originally anticipate, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

All processing must also be lawful, so you do need a lawful basis. The original basis you used to collect the data may not always be appropriate for your new use of that data.

If your new purpose is compatible, and your use of the data is necessary for that purpose, you can generally be confident it will also be lawful. In most cases, the appropriate basis for your new use of the data is likely to be fairly obvious. See our [lawful basis guidance](#) for more information.

However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful. See our [lawful basis guidance](#) for more information.

You need to make sure that you update your privacy information to ensure that your processing is transparent.

What is a ‘compatible’ purpose?

The UK GDPR specifically says that the following purposes should be considered to be compatible purposes:

- archiving purposes in the public interest;
- scientific or historical research purposes; and
- statistical purposes.

Please read our [detailed guidance on the research provisions](#) for more information.

Otherwise, you need to do a compatibility assessment to decide whether a new purpose is compatible with your original purpose. The assessment should take into account:

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – eg is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg encryption or pseudonymisation.

This list is not exhaustive and what you need to look at depends on the particular circumstances.

We consider a compatibility assessment is likely to look at similar factors to a legitimate interests assessment (LIA). Although there's no requirement to do so, you could therefore use our [LIA template](#) to help you assess compatibility.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose data for this type of purpose.

Example

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

Further Reading

 Key provisions in the UK GDPR - see Article 5(1)(b), Recital 39 (principles), Article 6(4) and Recital 50 (compatibility) and Article 30 (documentation) 
External link

Further reading

Read our guidance on:

- Documentation
- The right to be informed
- Lawful basis for processing
- The research provisions

Latest updates

07 October 2022 - We have updated our position on needing a new lawful basis when your purpose

Lawfulness, fairness and transparency

At a glance

- You must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

Checklist

Lawfulness

- We have identified an appropriate lawful basis (or bases) for our processing.
- If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.
- We don't do anything generally unlawful with personal data.

Fairness

- We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- We do not deceive or mislead people when we collect their personal data.

Transparency

- We are open and honest, and comply with the transparency obligations of the right to be informed.

In brief

- [What is the lawfulness, fairness and transparency principle?](#)
- [What is lawfulness?](#)

- [What is fairness?](#)
- [What is transparency?](#)

What is the lawfulness, fairness and transparency principle?

Article 5(1) of the UK GDPR says:

“

“1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')”

There are more detailed provisions on lawfulness and having a 'lawful basis for processing' set out in Articles 6 to 10.

There are more detailed transparency obligations set out in Articles 13 and 14, as part of the 'right to be informed'.

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

What is lawfulness?

For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis' for processing, and there are six options which depend on your purpose and your relationship with the individual. There are also specific additional conditions for processing some especially sensitive types of data. For more information, see the [lawful basis section of this guide](#).

If no lawful basis applies then your processing will be unlawful and in breach of this principle.

Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

These are just examples, and this list is not exhaustive. You may need to take your own legal advice on other relevant legal requirements.

Although processing personal data in breach of copyright or industry regulations (for example) will involve unlawful processing in breach of this principle, this does not mean that the ICO can pursue allegations which are primarily about breaches of copyright, financial regulations or other laws outside our remit and expertise as data protection regulator. In this situation there are likely to be other legal or regulatory routes of redress where the issues can be considered in a more appropriate forum.

If you have processed personal data unlawfully, the UK GDPR gives individuals the right to erase that data or restrict your processing of it.

What is fairness?

Processing of personal data must always be fair as well as lawful. If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.

Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.

Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified.

Example

Where personal data is collected to assess tax liability or to impose a fine for breaking the speed limit, the information is being used in a way that may cause detriment to the individuals concerned, but the proper use of personal data for these purposes will not be unfair.

You should also ensure that you treat individuals fairly when they seek to exercise their rights over their data. This ties in with your obligation to facilitate the exercise of individuals' rights. Read our guidance on rights for more information.

What is transparency?

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and

honest with people from the start about who you are, and how and why you use their personal data.

Transparency is always important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship.

Transparency is important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'.

You must ensure that you tell individuals about your processing in a way that is easily accessible and easy to understand. You must use clear and plain language.

For more detail on your transparency obligations and the privacy information you must provide to individuals, see our guidance on the [right to be informed](#).

Further Reading

↗ Relevant provisions in the UK GDPR - See Article 5(1)(a) and Recital 39 (principles), and Article 6 (lawful bases), Article 9 (special category data), Article 10 (criminal offences data) and Articles 13 and 14 (the right to be informed), Article 17(1)(d) (the right to erasure) ↗

External link

Further reading

Read our guidance on:

- [Lawful basis for processing](#)
- [The right to be informed](#)
- [Individuals' rights](#)

The [Accountability Framework](#) looks at the ICO's expectations in relation to transparency.

Lawful basis for processing

At a glance

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. We have an [interactive tool](#) to help you.
- Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you need to consider whether you need a new lawful basis.
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Checklist

- We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.
- We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose.
- We have documented our decision on which lawful basis applies to help us demonstrate compliance.
- We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- Where we process special category data, we have also identified a condition for processing special category data, and have documented this.
- Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

In brief

- What are the lawful bases for processing?
- When is processing 'necessary'?
- Why is the lawful basis for processing important?
- How do we decide which lawful basis applies?
- Is this different for public authorities?
- Can we change our lawful basis?
- What happens if we have a new purpose?
- How should we document our lawful basis?
- What do we need to tell people?
- What about special category data?
- What about criminal offence data?

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, read the specific page of this guide.

Further Reading

 Relevant provisions in the UK GDPR - See Article 6(1), Article 6(2) and Recital 40 

External link

When is processing 'necessary'?

Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of your chosen methods.

Why is the lawful basis for processing important?

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. If no lawful basis applies to your processing, your processing will be unlawful and in breach of the first principle.

Individuals also have the right to erase personal data which has been processed unlawfully.

The individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			✗ but right to withdraw consent
Contract			✗
Legal obligation	✗	✗	✗
Vital interests		✗	✗
Public task	✗	✗	
Legitimate interests		✗	

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

The remaining rights are not always absolute, and there are other rights which may be affected in other ways. For example, your lawful basis may affect how provisions relating to automated decisions and

profiling apply, and if you are relying on legitimate interests you need more detail in your privacy notice. Please read the section of this Guide on individuals' rights for full details.

Further Reading

 Relevant provisions in the UK GDPR - See Article 6 and Recitals 39, 40, and Chapter III (Rights of the data subject) 

External link

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should think about why you want to process the data, and consider which lawful basis best fits the circumstances. You can use our [interactive guidance tool](#) to help you.

You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the UK GDPR.

Several of the lawful bases relate to a particular specified purpose – a legal obligation, performing a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

In other cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.

In more detail

We have produced the [lawful basis interactive guidance tool](#), to give more tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Is this different for public authorities?

The basic approach is the same. You should think about your purposes, and choose whichever basis fits best. You can still use our [lawful basis tool](#) to help you.

The public task basis is more likely to be relevant to much of what you do. If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. But if it is for another purpose, you can still consider another basis.

In particular, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, although there are some limitations. For more information, see the specific guidance page on each lawful basis.

The Data Protection Act 2018 says that 'public authority' here means a public authority under the Freedom of Information Act or Freedom of Information (Scotland) Act – with the exception of parish and community councils.

Example

A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

Universities are classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances. For example, a University might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes.

The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

Further Reading

 [Key provisions in the Data Protection Act 2018 - See section 7 \(Meaning of 'public authority' and 'public body'\)](#) 

External link

Can we change our lawful basis?

You must determine your lawful basis before starting to process personal data. It's important to get this right first time. If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

Example

A company decided to process on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent.

It is therefore important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should make this clear from the start.

If there is a genuine change in circumstances or you have a new and unanticipated purpose which means there is a good reason to review your lawful basis and make a change, you need to inform the individual and document the change.

Further Reading

 Relevant provisions in the UK GDPR - See Article 6(1) and Recitals 39 and 40 

External link

What happens if we have a new purpose?

If your purposes change over time or you have a new purpose which you did not originally anticipate, you need to comply with the purpose limitation principle. In summary, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

For more information on compatibility, see our [purpose limitation guidance](#).

All processing must be lawful, so you also need to identify a lawful basis. The original basis you used to collect the data may not always be appropriate for your new use of the data.

In most cases, the appropriate basis for your new use of the data is likely to be fairly obvious. For example, if you are getting specific consent for the new purpose, your lawful basis will be consent. If you are relying on a legal provision requiring the new processing in the public interest, your lawful basis will be legal obligation. If you are relying on a legal provision allowing the new use of data in the public interest, your lawful basis will be public task.

Where the purpose for your new processing activity is compatible with the original purpose for the processing, you are likely to be able to rely on “legitimate interests” as the lawful basis for the new processing, provided your use of the personal data is necessary for that purpose.

We consider a compatibility assessment is likely to look at similar factors to a legitimate interests assessment (LIA). Although there’s no requirement to do so, you could therefore use our [LIA template](#) to help you assess compatibility. This will also help demonstrate your lawful basis at the same time.

If your new processing is for research purposes, you do not need to carry out a compatibility assessment, and in most circumstances you can be confident that your lawful basis is likely to be either public task or legitimate interests. See our guidance on the [research provisions](#) for more detail on this.

However, if you originally collected the data on the basis of consent, you should get fresh consent which specifically covers the new purpose (unless you are relying on a clear legal provision specifically permitting your reuse of the data). This is because consent means giving individuals real choice and control over how their data is used. This means that consent must always be specific and informed. People can only give valid consent when they know and understand what you are going to do with their data. If you do get specific consent for the new purpose, you do not need to show it is compatible.

If you are processing special category data, you will also need to ensure that you can identify an appropriate condition which applies to your new processing.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 6\(4\), Article 5\(1\)\(b\) and Recital 50, Recital 61](#) 
External link

How should we document our lawful basis?

The principle of accountability requires you to be able to demonstrate that you are complying with the UK GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular

processing purpose.

Read the accountability section of this guide for more on this topic. There is also further guidance on documenting consent or legitimate interests assessments in the relevant pages of the guide.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5(2) and 24 
External link

What do we need to tell people?

You need to include information about your lawful basis (or bases, if more than one applies) in your privacy notice. Under the transparency provisions of the UK GDPR, the information you need to give people includes:

- your intended purposes for processing the personal data; and
- the lawful basis for the processing.

This applies whether you collect the personal data directly from the individual or you collect their data from another source.

Read the 'right to be informed' section of this guide for more on the transparency requirements of the GDPR.

Further Reading

 Relevant provisions in the UK GDPR - See Article 13(1)(c), Article 14(1)(c) and Recital 39 (external link) 
External link

What about special category data?

If you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on [special category data](#).

What about criminal offence data?

If you are processing data about criminal convictions, criminal offences or related security measures, you need both a lawful basis for processing, and either 'official authority' or a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on [criminal offence data](#).

Criminal offence data

At a glance

- The UK GDPR gives extra protection to the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings.
- If you have official authority, you can process personal data about criminal convictions and offences, because you are processing the data in an official capacity.
- If you do not have official authority, you can only process criminal offence data if you can identify a specific condition for processing in Schedule 1 of the DPA 2018.
- You cannot keep a comprehensive register of criminal convictions, unless you do so in an official capacity.
- You must determine your condition for processing criminal offence data, or identify your official authority for the processing, before you begin the processing, and you should document this.
- You must still have a lawful basis for your processing under Article 6.
- In many cases, you also need an '[appropriate policy document](#)' in place in order to meet a UK Schedule 1 condition for processing in the DPA 2018.
- You need to complete a data protection impact assessment (DPIA) for any type of processing which is likely to be high risk. You must therefore be aware of the risks of processing the criminal offence data.

Checklist

- We have checked that the processing of the criminal offence data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve this purpose.
- We have identified an Article 6 lawful basis for processing the criminal offence data.
- Where applicable, we have identified in law our official authority to process the criminal offence data.
- Where we do not have official authority to process criminal offence data, we have identified an appropriate DPA 2018 Schedule 1 condition.
- Where required, we have an [appropriate policy document ↗](#).
- We have considered whether we need to do a DPIA.
- We include specific information about our processing of criminal offence data in our privacy information for individuals.
- We have considered whether the risks associated with our use of criminal offence data affect our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.

In brief

- [What is criminal offence data?](#)
- [What are the rules for criminal offence data?](#)
- [What are the Schedule 1 conditions for processing criminal offence data?](#)
- [In more detail](#)

What is criminal offence data?

The UK GDPR gives extra protection to “personal data relating to criminal convictions and offences or related security measures”. We refer to this as criminal offence data.

This covers a wide range of information about offenders or suspected offenders in the context of:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

It includes not just data which is obviously about a specific criminal conviction or trial, but may also include personal data about:

- unproven allegations; and
- information relating to the absence of convictions.

It also covers a wide range of related security measures, including

- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty if not adhered to.

It does not cover information about other individuals, including victims and witnesses of crime. However, information about victims and witnesses is likely to be sensitive, and controllers should take particular care when processing it.

What are the rules for criminal offence data?

You must always ensure that your processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the UK GDPR. To ensure that your processing is lawful, you need to identify an Article 6 basis for processing.

In addition, you can only process criminal offence data if the processing is either:

- [under the control of official authority](#); or
- authorised by domestic law. This means you need to meet one of the [conditions in Schedule 1](#) of the DPA 2018.

You may only keep a comprehensive register of criminal convictions if this register is “under the control of official authority”.

Public bodies, or private bodies who are given public sector tasks, may have “official authority” to process criminal offence data. This official authority may derive from either common law or statute. If you are a public body, you must identify the specific law that gives you official authority to process criminal offence data.

If you do not have official authority for the processing, it must be authorised by domestic law. This authorisation in law is set out in the conditions listed in [Schedule 1 of the DPA 2018](#).

You must also identify whether you need an “appropriate policy document” under the DPA 2018. Our [template appropriate policy document](#) shows the kind of information this should contain.

You must do a DPIA for any type of processing that is likely to be high risk. This means that you are more likely to need to do a DPIA for processing criminal offence data. For further information, please see our guidance on [DPIAs](#).

You should also consider how the risks associated with criminal offence data affect your other obligations – in particular, obligations around data minimisation, security, transparency, and DPOs.

What are the Schedule 1 conditions for processing criminal offence data?

The 28 conditions which are available for the processing of criminal offence data are set out in paragraphs 1

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

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

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

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

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

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

Special category data

At a glance

- Special category data is personal data that needs more protection because it is sensitive.
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked.
- There are 10 conditions for processing special category data in Article 9 of the UK GDPR.
- Five of these require you to meet additional conditions and safeguards set out in UK law, in Schedule 1 of the DPA 2018.
- You must determine your condition for processing special category data before you begin this processing under the UK GDPR, and you should document it.
- In many cases you also need an '[appropriate policy document](#)' in place in order to meet a UK Schedule 1 condition for processing in the DPA 2018.
- You need to complete a data protection impact assessment (DPIA) for any type of processing which is likely to be high risk. You must therefore be aware of the risks of processing the special category data.

Checklist

- We have checked the processing of the special category data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.
- We have identified an Article 6 lawful basis for processing the special category data.
- We have identified an appropriate Article 9 condition for processing the special category data.
- Where required, we have also identified an appropriate DPA 2018 Schedule 1 condition.
- We have documented which special categories of data we are processing.
- Where required, we have an [appropriate policy document](#) in place.
- We have considered whether we need to do a DPIA.
- We include specific information about our processing of special category data in our privacy information for individuals.
- If we use special category data for automated decision making (including profiling), we have checked we comply with Article 22.
- We have considered whether the risks associated with our use of special category data affect our

other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.

In brief

- [What is special category data?](#)
- [What are the rules for special category data?](#)
- [What are the conditions for processing special category data?](#)
- [What are the substantial public interest conditions?](#)
- [In more detail](#)

What is special category data?

The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply. For further information, please see our separate guidance on [criminal offence data](#).

Special category data includes personal data **revealing or concerning** the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

What are the rules for special category data?

You must always ensure that your processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the UK GDPR. To ensure that your processing is lawful, you need to identify an Article 6 basis for processing.

In addition, you can only process special category data if you can meet one of the specific conditions in Article 9 of the UK GDPR. You need to consider the purposes of your processing and identify which of these conditions are relevant.

Five of the conditions for processing are provided solely in Article 9 of the UK GDPR. The other five require authorisation or a basis in UK law, which means you need to meet additional conditions set out in the DPA 2018.

You must also identify whether you need an 'appropriate policy document' under the DPA 2018. Our [template appropriate policy document](#) shows the kind of information this should contain.

You must do a DPIA for any type of processing that is likely to be high risk. This means that you are more likely to need to do a DPIA for processing special category data. For further information, please see our guidance on [DPIAs](#).

If you process special category data you must keep records, including documenting the categories of data. You may also need to consider how the risks associated with special category data affect your other obligations – in particular, obligations around data minimisation, security, transparency, DPOs and rights related to automated decision-making.

What are the conditions for processing special category data?

Article 9 lists the conditions for processing special category data:

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of [Schedule 1 of the DPA 2018](#).

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

What are the substantial public interest conditions?

The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements

13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

You should identify which of these conditions appears to most closely reflect your purpose. Our detailed guidance gives you some further advice on how the conditions generally work, but you always need to refer to the [detailed provisions of each condition](#) in the legislation itself to make sure you can demonstrate it applies.

For some of these conditions, the substantial public interest element is built in. For others, you need to be able to demonstrate that your specific processing is “necessary for reasons of substantial public interest”, on a case-by-case basis.

The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. It needs to be real and of substance. Given the inherent risks of special category data, it is not enough to make a vague or generic public interest argument. You should be able to make specific arguments about the concrete wider benefits of your processing.

For some of the conditions, you also need to justify why you cannot give individuals a choice and get explicit consent for your processing. In most cases, you must have an '[appropriate policy document](#)' in place.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 4\(1\), 4\(13\)-\(15\) and Recitals 34 and 35, see also Articles 6 and 9, and Recitals 51 and 54, and Articles 22\(4\), 27\(2\), 30\(5\), 35\(3\), 37\(1\)](#) 
External link

 [Key provisions in the DPA 2018 - See sections 10 and 11, and schedule 1](#) 
External link

Legitimate interests

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
 - identify a legitimate interest;
 - show that the processing is necessary to achieve it; and
 - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Checklists

- We have checked that legitimate interests is the most appropriate basis.
- We understand our responsibility to protect the individual's interests.
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
- We have identified the relevant legitimate interests.
- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
- We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If we process children's data, we take extra care to make sure we protect their interests.
- We have considered safeguards to reduce the impact where possible.
- We have considered whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
- We keep our LIA under review, and repeat it if circumstances change.
- We include information about our legitimate interests in our privacy information.

In brief

- [What is the 'legitimate interests' basis?](#)
- [When can we rely on legitimate interests?](#)
- [How can we apply legitimate interests in practice?](#)
- [What else do we need to consider?](#)
- [In detail](#)

What is the 'legitimate interests' basis?

Article 6(1)(f) gives you a lawful basis for processing where:

“

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?

2. **Necessity test:** is the processing necessary for that purpose?

3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The UK GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can we rely on legitimate interests?

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our [Guide to PECR](#) for more on when you need consent for electronic marketing.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See our detailed guidance on [children and the UK GDPR](#).

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You

should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

See our [guidance page on the lawful basis](#) for more information on the alternatives to legitimate interests, and how to decide which basis to choose.

How can we apply legitimate interests in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?

- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our [guidance on DPIAs](#) for more on this.

What else do we need to consider?

You must tell people in your privacy information that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights. See our guidance on [individual rights](#) for more on this.

Our [legitimate interests assessment \(LIA\) template](#) is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 6\(1\)\(f\) and Recitals 47 - 49](#) 

External link

Public task

At a glance

- You can rely on this lawful basis if you need to process personal data:
 - 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
 - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

In brief

- What is the 'public task' basis?
- What does 'laid down by law' mean?
- Who can rely on this basis?
- When can we rely on this basis?
- What else should we consider?

What is the 'public task' basis?

Article 6(1)(e) gives you a lawful basis for processing where:

“

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

In this guide we use the term 'public task' to help describe and label this lawful basis. However, this is not a term used in the UK GDPR itself. Your focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority.

In particular, there is no direct link to the concept of 'public task' in the Re-use of Public Sector Information Regulations 2015 (RPSI). There is some overlap, as a public sector body's core role and functions for RPSI purposes may be a useful starting point in demonstrating official authority for these purposes. However, you shouldn't assume that it is an identical test. See our [Guide to RPSI](#) for more on public task in the context of RPSI.

What does 'laid down by law' mean?

Article 6(3) requires that the relevant task or authority must be laid down by domestic law. This will most often be a statutory function. However, Recital 41 clarifies that this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law.

Who can rely on this basis?

Any controller who is exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Act 2018. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest. See our guidance on [Public authorities under the EIR](#) for more details.

However, if you are a private sector organisation you are likely to be able to consider the legitimate interests basis as an alternative.

See the main lawful basis page of this guide for more on how to choose the most appropriate basis.

When can we rely on this basis?

Section 8 of the Data Protection Act 2018 (DPA 2018) says that the public task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions;
- governmental functions; or
- activities that support or promote democratic engagement.

However, this is not intended as an exhaustive list. If you have other official non-statutory functions or public interest tasks you can still rely on the public task basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other reasonable and less intrusive means to achieve your purpose.

You may share personal information with another controller or individual in the lawful exercise of any of your public tasks, functions or powers, if it is a clear and foreseeable use of the information. In order to do so, you should be able to identify the relevant legal basis you are subject to.

However, you cannot rely on another controller's public tasks, functions or powers as the lawful basis for your processing, including disclosing personal data to them, as this is not a clear and foreseeable use of the information.

Example

A government agency has statutory powers to conduct research about the online shopping habits of consumers. The agency asks retailers to share the personal data of a random sample of their customers to enable it to carry out this function. It explains that it will process the data under 'public task' once it receives the information.

As the retailers are not subject to the agency's statutory function, they cannot share the information on the basis of the agency's public task. However, they may consider disclosing the information under another lawful basis, eg legitimate interests.

What else should we consider?

Individuals' rights to erasure and data portability do not apply if you are processing on the basis of public

task. However, individuals do have a right to object. See our guidance on individual rights for more information.

You should consider an alternative lawful basis if you are not confident that processing is necessary for a relevant task, function or power which is clearly set out in law.

If you are a public authority (as defined in the Data Protection Act 2018), your ability to rely on consent or legitimate interests as an alternative basis is more limited, but they may be available in some circumstances. In particular, legitimate interests is still available for processing which falls outside your tasks as a public authority. Other lawful bases may also be relevant. See our guidance on the other lawful bases for more information.

Remember that the UK GDPR specifically says that further processing for certain purposes should be considered to be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing for:

- archiving purposes in the public interest;
- scientific research purposes; or
- statistical purposes.

If you are processing special category data, you also need to identify an additional condition for processing this type of data. The Data Protection Act 2018 includes specific conditions for parliamentary, statutory or governmental functions in the substantial public interest. Read the special category data page of this guide for our latest guidance on these provisions.

To help you meet your accountability and transparency obligations, remember to:

- document your decision that the processing is necessary for you to perform a task in the public interest or exercise your official authority;
- identify the relevant task or authority and its basis in common law or statute; and
- include basic information about your purposes and lawful basis in your privacy notice.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 6\(1\)\(e\) and 6\(3\), and Recitals 41, 45 and 50](#) 
External link

 [Relevant provisions in the Data Protection Act 2018 - See sections 7 and 8, and Schedule 1 paras 6 and 7](#) 
External link

Vital interests

At a glance

- You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

In brief

- [What does the UK GDPR say?](#)
- [What are 'vital interests'?](#)
- [When is the vital interests basis likely to apply?](#)
- [What else should we consider?](#)

What does the UK GDPR say?

Article 6(1)(d) provides a lawful basis for processing where:

“

“processing is necessary in order to protect the vital interests of the data subject or of another natural person”.

Recital 46 provides some further guidance:

“

“The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis...”

What are 'vital interests'?

It's clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

When is the vital interests basis likely to apply?

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as public task or legitimate interests is likely to be more appropriate in this case.

Processing of one individual's personal data to protect the vital interests of others is likely to happen more rarely. It may be relevant, for example, if it is necessary to process a parent's personal data to protect the vital interests of a child.

Vital interests is also less likely to be the appropriate basis for processing on a larger scale. Recital 46 does suggest that vital interests might apply where you are processing on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

However, if you are processing one person's personal data to protect someone else's life, Recital 46 also indicates that you should generally try to use an alternative lawful basis, unless none is obviously available. For example, in many cases you could consider legitimate interests, which will give you a framework to balance the rights and interests of the data subject(s) with the vital interests of the person or people you are trying to protect.

What else should we consider?

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means you will also need to identify a condition for processing special category data under Article 9.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you cannot in practice rely on vital interests for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Legal obligation

At a glance

- You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

In brief

- [What does the UK GDPR say?](#)
- [When is the lawful basis for legal obligations likely to apply?](#)
- [When is processing 'necessary' for compliance?](#)
- [What else should we consider?](#)

What does the UK GDPR say?

Article 6(1)(c) provides a lawful basis for processing where:

“

“processing is necessary for compliance with a legal obligation to which the controller is subject.”

When is the lawful basis for legal obligations likely to apply?

In short, when you are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision

or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

Example

A financial institution relies on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 to process personal data in order submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering.

Example

A court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation.

Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

Example

The Competition and Markets Authority (CMA) has powers under The Enterprise Act 2002 to make orders to remedy adverse effects on competition, some of which may require the processing of personal data.

A retail energy supplier passes customer data to the Gas and Electricity Markets Authority to comply with the CMA's Energy Market Investigation (Database) Order 2016. The supplier may rely on legal obligation as the lawful basis for this processing.

A contractual obligation does not comprise a legal obligation in this context. You cannot contract out of the requirement for a lawful basis. However, you can look for a different lawful basis. If the contract is with the individual you can consider the lawful basis for contracts. For contracts with other parties, you may want to consider legitimate interests.

When is processing ‘necessary’ for compliance?

Although the processing need not be essential for you to comply with the legal obligation, it must be a reasonable and proportionate way of achieving compliance. You cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply.

It is likely to be clear from the law in question whether the processing is actually necessary for compliance.

What else should we consider?

If you are processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Read our guidance on individual rights for more information.

Remember to:

- document your decision that processing is necessary for compliance with a legal obligation;
- identify an appropriate source for the obligation in question; and
- include information about your purposes and lawful basis in your privacy notice.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 6\(1\)\(c\), Recitals 41, 45](#) 
External link

In more detail - ICO guidance

Contract

At a glance

- You can rely on this lawful basis if you need to process someone's personal data:
 - to deliver a contractual service to them; or
 - because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want by processing less data, or using their data in a less intrusive way, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

In brief

- [When is the lawful basis for contracts likely to apply?](#)
- [When is processing 'necessary' for a contract?](#)
- [What else should we consider?](#)

When is the lawful basis for contracts likely to apply?

You have a lawful basis for processing if:

- you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
- you have a contract with the individual and you need to process their personal data so that they can comply with specific counter-obligations under the contract (eg you are processing payment details).
- you haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask. This applies even if they don't actually go on to enter into a contract with you, as long as the processing was in the context of a potential contract with that individual.

Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

It does not apply if you need to process one person's details but the contract is with someone else.

It does not apply if you collect and reuse your customer's data for your own business purposes, even if this is permitted under your standard contractual terms and is part of your funding model.

It does not apply if you take pre-contractual steps on your own initiative, to meet other obligations, or at the request of a third party.

Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt you should seek your own legal advice.

When is processing ‘necessary’ for a contract?

‘Necessary’ does not mean that the processing must be absolutely essential or ‘the only way’ to perform the contract or take relevant pre-contractual steps. However, it must be more than just useful, and more than just part of your standard terms. It must be a targeted and proportionate step which is integral to delivering the contractual service or taking the requested action. This lawful basis does not apply if there are other reasonable and less intrusive ways to deliver the contractual service or take the steps requested.

The processing must be necessary to perform the contract with this particular person. If the processing is instead necessary to maintain your business model more generally, or is included in your terms for other business purposes beyond delivering the contractual service, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

Example

When a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

However, the profiling of an individual’s interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on Article 6(1)(b) as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your customer relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis (and other safeguards such as the right to object may come into play).

What else should we consider?

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent.

If processing of special category data is necessary for the contract, you also need to identify a separate condition for processing this data. Read our guidance on [special category data](#) for more information.

If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected. Read our guidance on [children and the GDPR](#) for more information.

If the processing is not necessary for the contract, you need to consider another lawful basis such as legitimate interests or consent. Note that if you want to rely on consent you will not generally be able to make the processing a condition of the contract. Read our guidance on [consent](#) for more information.

If you are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability. Read our guidance on [individual rights](#) for more information.

Remember to document your decision that processing is necessary for the contract, and include information about your purposes and lawful basis in your privacy notice.

Further Reading

 Relevant provisions in the UK GDPR - See Article 6(1)(b) and Recital 44 

External link

In more detail – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB has adopted [final guidelines](#) on processing under Article 6(1)(b) in the context of online services. EDPB guidelines are no longer be directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Consent

At a glance

- The UK GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the UK GDPR standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

Checklists

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don't penalise individuals who wish to withdraw consent.

In brief

- [Why is consent important?](#)
- [When is consent appropriate?](#)
- [What is valid consent?](#)

- How should we obtain, record and manage consent?
- In detail

Why is consent important?

The UK GDPR sets a high standard for consent, which must be unambiguous and involve a clear affirmative action (an opt-in).

It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The UK GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the UK GDPR standard. If they do, there is no need to obtain fresh consent.

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to large fines.

When is consent appropriate?

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

What is valid consent?

Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should we obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 4(11), 6(1)(a) 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 171 

External link

In more detail - ICO guidance

We have produced more detailed guidance on [consent](#).

We have produced [an interactive guidance tool](#) to give tailored guidance on which lawful basis is likely

Individual rights

The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the guide explains these rights.

Rights related to automated decision making including profiling

At a glance

- The UK GDPR has provisions on:
 - automated individual decision-making (making a decision solely by automated means without any human involvement); and
 - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The UK GDPR applies to all automated individual decision-making and profiling.
- Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is:
 - necessary for the entry into or performance of a contract; or
 - authorised by domestic law applicable to the controller; or
 - based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
 - give individuals information about the processing;
 - introduce simple ways for them to request human intervention or challenge a decision;
 - carry out regular checks to make sure that your systems are working as intended.

Checklists

All automated individual decision-making and profiling

To comply with the UK GDPR...

- We have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.
- We send individuals a link to our privacy statement when we have obtained their personal data indirectly.
- We explain how people can access details of the information we used to create their profile.
- We tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes.
- We have procedures for customers to access the personal data input into the profiles so they can

review and edit for any accuracy issues.

- We have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children).
- We only collect the minimum amount of data needed and have a clear retention policy for the profiles we create.

As a model of best practice...

- We carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling.
- We tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.
- We use anonymised data in our profiling activities.

Solely automated individual decision-making, including profiling with legal or similarly significant effects (Article 22)

To comply with the UK GDPR...

- We carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to meet UK GDPR requirements.
- We carry out processing under Article 22(1) for contractual purposes and we can demonstrate why it's necessary.

OR

- We carry out processing under Article 22(1) because we have the individual's explicit consent recorded. We can show when and how we obtained consent. We tell individuals how they can withdraw consent and have a simple way for them to do this.

OR

- We carry out processing under Article 22(1) because we are authorised or required to do so. This is the most appropriate way to achieve our aims.
- We don't use special category data in our automated decision-making systems unless we have a lawful basis to do so, and we can demonstrate what that basis is. We delete any special category data accidentally created.
- We explain that we use automated decision-making processes, including profiling. We explain what information we use, why we use it and what the effects might be.
- We have a simple way for people to ask us to reconsider an automated decision.

We have identified staff in our organisation who are authorised to carry out reviews and change decisions.

We regularly check our systems for accuracy and bias and feed any changes back into the design process.

As a model of best practice...

We use visuals to explain what information we collect/use and why this is relevant to the process.

We have signed up to [standard] a set of ethical principles to build trust with our customers. This is available on our website and on paper.

In brief

- [What is automated individual decision-making and profiling?](#)
- [What does the GDPR say about automated individual decision-making and profiling?](#)
- [When can we carry out this type of processing?](#)
- [What else do we need to consider?](#)
- [What if Article 22 doesn't apply to our processing?](#)
- [In detail](#)

What is automated individual decision-making and profiling?

Automated individual decision-making is a decision made by automated means without any human involvement.

Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do.

The UK GDPR says that profiling is:

“

“Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

[Article 4(4)]

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. There is more information about algorithms and machine-learning in our paper on [big data, artificial intelligence, machine learning and data protection](#).

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about individuals’ preferences;
- predict their behaviour; and/or
- make decisions about them.

This can be very useful for organisations and individuals in many sectors, including healthcare, education, financial services and marketing.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The UK GDPR provisions are designed to address these risks.

What does the UK GDPR say about automated individual decision-making and profiling?

The UK GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

“

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

[Article 22(1)]

For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the UK GDPR, but the decision must have a serious impact on an individual to be caught by this provision.

A legal effect is something that affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

When can we carry out this type of processing?

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.

You can **only** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If you're using special category personal data you can **only** carry out processing described in Article 22(1) if:

- you have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

What else do we need to consider?

Because this type of processing is considered to be high-risk the UK GDPR requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them.

As well as restricting the circumstances in which you can carry out solely automated individual decision-making (as described in Article 22(1)) the UK GDPR also:

- requires you to give individuals specific information about the processing;
- obliges you to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision.

These provisions are designed to increase individuals' understanding of how you might be using their personal data.

You must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;

- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
 - obtain human intervention;
 - express their point of view; and
 - obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors;
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

What if Article 22 doesn't apply to our processing?

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

But you must still comply with the UK GDPR principles.

You must identify and record your [lawful basis for the processing](#).

You need to have processes in place so people can [exercise their rights](#).

Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Further Reading

 [Relevant provisions in the UK GDPR - Article 4\(4\), 9, 12, 13, 14, 15, 21, 22, 35\(1\)and \(3\)](#) 
External link

In more detail – ICO guidance

- We have published detailed guidance on [automated decision-making and profiling](#).
- [Privacy notices transparency and control](#)
- [Big data, artificial intelligence, machine learning and data protection](#) 

In more detail – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

Right to object

At a glance

- The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one calendar month to respond to an objection.

Checklists

Preparing for objections to processing

- We know how to recognise an objection and we understand when the right applies.
- We have a policy in place for how to record objections we receive verbally.
- We understand when we can refuse an objection and are aware of the information we need to provide to individuals when we do so.
- We have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.
- We understand when we need to inform individuals of their right to object in addition to including it in our privacy notice.

Complying with requests which object to processing

- We have processes in place to ensure that we respond to an objection without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to an objection.
- We have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

In brief

- What is the right to object?
- When does the right to object apply?
- Direct marketing
- Processing based upon public task or legitimate interests
- Do we need to tell individuals about the right to object?
- Do we always need to erase personal data to comply with an objection?
- Can we refuse to comply with an objection for other reasons?
- What does manifestly unfounded mean?
- What does excessive mean?
- What should we do if we refuse to comply with an objection?
- How do we recognise an objection?
- Can we charge a fee?
- How long do we have to comply?
- Can we extend the time for a response?
- Can we ask an individual for ID?

What is the right to object?

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data.

An objection may be in relation to all of the personal data you hold about an individual or only to certain information. It may also only relate to a particular purpose you are processing the data for.

When does the right to object apply?

The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If you are processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

These various grounds are discussed further below.

Direct marketing

An individual can object to the processing of their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing, you must not process the individual's data for this purpose.

However, this does not automatically mean that you need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

Processing based upon public task or legitimate interests

An individual can also object where you are relying on one of the following lawful bases:

- 'public task' (for the performance of a task carried out in the public interest),
- 'public task' (for the exercise of official authority vested in you), or
- legitimate interests.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

In these circumstances this is not an absolute right, and you can refuse to comply if:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (eg the processing is causing them financial loss), the grounds for their objection will have more weight. In making a decision on this, you need to balance the individual's interests, rights and freedoms with your own legitimate grounds. During this process you should remember that the responsibility is for you to be able to demonstrate that your legitimate grounds override those of the individual.

If you are satisfied that you do not need to comply with the request you should let the individual know. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

Research purposes

Where you are processing personal data for scientific or historical research, or statistical purposes, the right to object is more restricted.

Article 21(6) states:

“

'Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her personal situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.'

Effectively this means that if you are processing data for these purposes and have appropriate safeguards in place (eg data minimisation and pseudonymisation where possible) the individual only has a right to object if your lawful basis for processing is:

- public task (on the basis that it is necessary for the exercise of official authority vested in you), or
- legitimate interests.

The individual does not have a right to object if your lawful basis for processing is public task because it is necessary for the performance of a task carried out in the public interest.

Article 21(6) therefore differentiates between the two parts of the [public task lawful basis](#) (performance of a task carried out in the public interest **or** in the exercise of official authority vested in you).

This may cause difficulties if you are relying on the public task lawful basis for processing. It may not always be clear whether you are carrying out the processing solely as a task in the public interest, or in the exercise of official authority. Indeed, it may be difficult to differentiate between the two.

As such, it is good practice that if you are relying upon the public task lawful basis and receive an objection, you should consider the objection on its own merits and go on to consider the steps outlined in the next paragraph, rather than refusing it outright. If you do intend to refuse an objection on the basis that you are carrying out research or statistical work solely for the performance of a public task carried out in the public interest you should be clear in your privacy notice that you are only carrying out this processing on this basis.

If you do receive an objection you may be able to continue processing, if you can demonstrate that you have a compelling legitimate reason or the processing is necessary for legal claims. You need to go through the steps outlined in the previous section to demonstrate this.

As noted above, if you are satisfied that you do not need to comply with the request you should let the individual know. You should provide an explanation for your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority, as well as their ability to seek to enforce their rights through a judicial remedy.

Do we need to tell individuals about the right to object?

The UK GDPR is clear that you must inform individuals of their right to object at the latest at the time of your first communication with them where:

- you process personal data for direct marketing purposes, or
- your lawful basis for processing is:

- public task (for the performance of a task carried out in the public interest),
- public task (for the exercise of official authority vested in you), or
- legitimate interests.

If one of these conditions applies, you should explicitly bring the right to object to the individual's attention. You should present this information clearly and separately from any other information.

If you are processing personal data for research or statistical purposes you should include information about the right to object (along with information about the other rights of the individual) in your privacy notice.

Do we always need to erase personal data to comply with an objection?

Where you have received an objection to the processing of personal data and you have no grounds to refuse, you need to stop or not begin processing the data.

This may mean that you need to erase personal data as the definition of processing under the UK GDPR is broad, and includes storing data. However, as noted above, this will not always be the most appropriate action to take.

Erasure may not be appropriate if you process the data for other purposes as you need to retain the data for those purposes. For example, when an individual objects to the processing of their data for direct marketing, you can place their details onto a suppression list to ensure that you continue to comply with their objection. However, you need to ensure that the data is clearly marked so that it is not processed for purposes the individual has objected to.

Can we refuse to comply with an objection for other reasons?

If an exemption applies, you can refuse to comply with an objection (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information, please see our guidance on [Exemptions](#).

You can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

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

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right to object. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
 - 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 sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word “manifestly” means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

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?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- makes a request about the same issue. 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;

- makes an overlapping request, if it relates to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

What should we do if we refuse to comply with an objection?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- 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.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise an objection?

The UK GDPR does not specify how to make a valid objection. Therefore, an objection to processing can be made verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'objection to processing' or Article 21 of the UK GDPR - as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal objection. However, you have a legal responsibility to identify that an individual has made an objection to you and to handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify an objection.

Additionally, it is good practice to have a policy for recording details of the objections 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 about how you have interpreted the objection. We also recommend that you keep a log of verbal objections.

Can we charge a fee?

In most cases you cannot charge a fee to comply with an objection.

However, you can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive. You should base the reasonable fee on the administrative costs of complying with the request.

If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request.

How long do we have to comply?

You must comply with an objection without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:

- any information requested to confirm the requester's identity (see [Can we ask an individual for ID?](#)); or
- a fee (only in certain circumstances – see [Can we charge a fee?](#))

You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

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 have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the objection you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their objection. The period for responding to the objection begins when you receive the additional information.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 6, 12, 21, 89 and Recitals 69 and 70 
External link

Further reading – ICO guidance

The [Accountability Framework](#) looks at the ICO's expectations in relation to the right to object.

Right to data portability

At a glance

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

Checklists

Preparing for requests for data portability

- We know how to recognise a request for data portability and we understand when the right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for data portability

- We can transmit personal data in structured, commonly used and machine readable formats.
- We use secure methods to transmit personal data.
- We have processes in place to ensure that we respond to a request for data portability without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.

In brief

- [What is the right to data portability?](#)
- [When does the right apply?](#)

- What does the right apply to?
- What does ‘provided to a controller’ mean?
- Does the right apply to anonymous or pseudonymous data?
- What happens if the personal data includes information about others?
- What is an individual entitled to?
- What are the limits when transmitting personal data to another controller?
- Do we have responsibility for the personal data we transmit to others?
- How should we provide the data?
- What does ‘structured’ mean?
- What does ‘commonly used’ mean?
- What does ‘machine-readable’ mean?
- Should we use an ‘interoperable’ format?
- What formats can we use?
- What is CSV?
- What is XML?
- What is JSON?
- Are these the only formats we can use?
- What responsibilities do we have when we receive personal data because of a data portability request?
- When can we refuse to comply with a request for data portability?
- What does manifestly unfounded mean?
- What does excessive mean?
- What should we do if we refuse to comply with a request for data portability?
- How do we recognise a request?
- Can we charge a fee?
- How long do we have to comply?
- Can we extend the time for a response?
- Can we ask an individual for ID?

What is the right to data portability?

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

When does the right apply?

The right to data portability only applies when:

- your lawful basis for processing this information is consent **or** for the performance of a contract; and
- you are carrying out the processing by automated means (ie excluding paper files).

What does the right apply to?

Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you.

What does 'provided to a controller' mean?

Sometimes the personal data an individual has provided to you will be easy to identify (eg their mailing address, username, age). However, the meaning of data 'provided to' you is not limited to this. It is also personal data resulting from observation of an individual's activities (eg where using a device or service).

This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices.

It does not include any additional data that you have created based on the data an individual has provided to you. For example, if you use the data they have provided to create a user profile then this data would not be in scope of data portability.

You should however note that if this 'inferred' or 'derived' data is personal data, you still need to provide it to an individual if they make a subject access request. Bearing this in mind, if it is clear that the individual is seeking access to the inferred/derived data, as part of a wider portability request, it would be good practice to include this data in your response.

Does the right apply to anonymous or pseudonymous data?

The right to data portability only applies to personal data. This means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to an individual (eg where that individual provides the respective identifier) is within scope of the right.

What happens if the personal data includes information about others?

If the requested information includes information about others (eg third party data) you need to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties.

Generally speaking, providing third party data to the individual making the portability request should not be a problem, assuming that the requestor provided this data to you within their information in the first place. However, you should always consider whether there will be an adverse effect on the rights and freedoms of third parties, in particular when you are transmitting data directly to another controller.

If the requested data has been provided to you by multiple data subjects (eg a joint bank account) you need to be satisfied that all parties agree to the portability request. This means that you may have to seek agreement from all the parties involved.

What is an individual entitled to?

The right to data portability entitles an individual to:

- receive a copy of their personal data; and/or
- have their personal data transmitted from one controller to another controller.

Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store.

You can achieve this by either:

- directly transmitting the requested data to the individual; or
- providing access to an automated tool that allows the individual to extract the requested data themselves.

This does not create an obligation for you to allow individuals more general and routine access to your systems – only for the extraction of their data following a portability request.

You may have a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, you need to ensure that the method is secure.

What are the limits when transmitting personal data to another controller?

Individuals have the right to ask you to transmit their personal data directly to another controller without hindrance. If it is technically feasible, you should do this.

You should consider the **technical feasibility** of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations (UK GDPR Recital 68). However, you should take a reasonable approach, and this should not generally create a barrier to transmission.

Without hindrance means that you should not put in place any legal, technical or financial obstacles which slow down or prevent the transmission of the personal data to the individual, or to another organisation.

However, there may be legitimate reasons why you cannot undertake the transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is however your responsibility to justify why these reasons are legitimate and why they are not a 'hindrance' to the transmission.

Do we have responsibility for the personal data we transmit to others?

If you provide information directly to an individual or to another organisation in response to a data portability request, you are not responsible for any subsequent processing carried out by the individual or the other organisation. However, you are responsible for the transmission of the data and need to take appropriate measures to ensure that it is transmitted securely and to the right destination.

If you provide data to an individual, it is possible that they will store the information in a system with less security than your own. Therefore, you should make individuals aware of this so that they can take steps to protect the information they have received.

You also need to ensure that you comply with the other provisions in the UK GDPR. For example, whilst there is no specific obligation under the right to data portability to check and verify the quality of the data you transmit, you should already have taken reasonable steps to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the UK GDPR.

How should we provide the data?

You should provide the personal data in a format that is:

- structured;
- commonly used; and
- machine-readable.

Although these terms are not defined in the UK GDPR these three characteristics can help you decide whether the format you intend to use is appropriate.

You can also find relevant information in the 'Open Data Handbook', published by Open Knowledge International. The handbook is a guide to 'open data', information that is free to access and can be re-used for any purpose – particularly information held by the public sector. The handbook contains a number of definitions that are relevant to the right to data portability, and this guidance includes some of these below.

What does 'structured' mean?

Structured data allows for easier transfer and increased usability.

The Open Data Handbook defines 'structured data' as:

“

'data where the structural relation between elements is explicit in the way the data is stored on a computer disk.'

This means that software must be able to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns, ie it is 'structured'. In practice, some of the personal data you process will already be in structured form.

In many cases, if a format is structured it is also machine-readable.

What does 'commonly used' mean?

This simply means that the format you choose must be widely-used and well-established.

However, just because a format is 'commonly used' does not mean it is appropriate for data portability. You have to consider whether it is 'structured', and 'machine-readable' as well. Although you may be using common software applications, which save data in commonly-used formats, these may not be sufficient to meet the requirements of data portability.

What does ‘machine-readable’ mean?

The Open Data Handbook states that ‘machine readable’ data is:

“

‘Data in a data format that can be automatically read and processed by a computer.’

Furthermore, Regulation 2 of the Re-use of Public Sector Information Regulations 2015 defines ‘machine-readable format’ as:

“

‘A file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure.’

Machine-readable data can be made directly available to applications that request that data over the web. This is undertaken by means of an application programming interface (“API”).

If you are able to implement such a system then you can facilitate data exchanges with individuals and respond to data portability requests in an easy manner.

Should we use an ‘interoperable’ format?

Although you are not required to use an interoperable format, this is encouraged by the UK GDPR, which seeks to promote the concept of interoperability. Recital 68 says:

“

‘Data controllers should be encouraged to develop interoperable formats that enable data portability.’

Interoperability allows different systems to share information and resources. An ‘interoperable format’ is a type of format that allows data to be exchanged between different systems and be understandable to both.

At the same time, you are not expected to maintain systems that are technically compatible with those of other organisations. Data portability is intended to produce interoperable systems, not compatible ones.

What formats can we use?

You may already be using an appropriate format within your networks and systems, and/or you may be required to use a particular format due to the particular industry or sector you are part of. Provided it meets the requirements of being structured, commonly-used and machine readable then it could be appropriate for a data portability request.

The UK GDPR does not require you to use open formats internally. Your processing systems may indeed use proprietary formats which individuals may not be able to access if you provide data to them in these formats. In these cases you need to perform some additional processing on the personal data in order to put it into the type of format required by the UK GDPR.

Where no specific format is in common use within your industry or sector, you should provide personal data using open formats such as CSV, XML and JSON. You may also find that these formats are the easiest for you to use when answering data portability requests.

For further information on CSV, XML and JSON, please see below.

What is CSV?

CSV stands for 'Comma Separated Values'. It is defined by the Open Data Handbook as:

“

'a standard format for spreadsheet data. Data is represented in a plain text file, with each data row on a new line and commas separating the values on each row. As a very simple open format it is easy to consume and is widely used for publishing open data.'

CSV is used to exchange data and is widely supported by software applications. Although CSV is not standardised it is nevertheless structured, commonly used and machine-readable and is therefore an appropriate format for you to use when responding to a data portability request.

What is XML?

XML stands for 'Extensible Markup Language'. It is defined by the Open Data Handbook as:

“

'a simple and powerful standard for representing structured data.'

It is a file format that is intended to be both human readable and machine-readable. Unlike CSV, XML is defined by a set of open standards maintained by the World Wide Web Consortium ("W3C"). It is widely used for documents, but can also be used to represent data structures such as those used in web services.

This means XML can be processed by APIs, facilitating data exchange. For example, you may develop or implement an API to exchange personal data in XML format with another organisation. In the context of data portability, this can allow you to transmit personal data to an individual's personal data store, or to another organisation if the individual has asked you to do so.

What is JSON?

JSON stands for 'JavaScript Object Notation'. The Open Data Handbook defines JSON as:

“

‘a simple but powerful format for data. It can describe complex data structures, is highly machine-readable as well as reasonably human-readable, and is independent of platform and programming language, and is therefore a popular format for data interchange between programs and systems.’

It is a file format based on the JavaScript language that many web sites use and is used as a data interchange format. As with XML, it can be read by humans or machines. It is also a standardised open format maintained by the W3C.

Are these the only formats we can use?

CSV, XML and JSON are three examples of structured, commonly used and machine-readable formats that are appropriate for data portability. However, this does not mean you are obliged to use them. Other formats exist that also meet the requirements of data portability.

Example

The RDF or ‘Resource Description Framework’ format is also a structured, commonly-used, machine-readable format. It is an open standard published by the W3C and is intended to provide interoperability between applications exchanging information.

You should however consider the nature of the portability request. If the individual cannot make use of the format, even if it is structured, commonly-used and machine-readable then the data will be of no use to them.

Further reading

The Open Data Handbook is published by Open Knowledge International and is a guide to 'open data'. The Handbook is updated regularly and you can read it here:

<http://opendatahandbook.org>

W3C candidate recommendation for XML is available here:

<http://www.w3.org/TR/2008/REC-xml-20081126/>

W3C's specification of the JSON data interchange format is available here:

<https://tools.ietf.org/html/rfc7159>

W3C's list of specifications for RDF is available here:

http://www.w3.org/standards/techs/rdf#w3c_all

What responsibilities do we have when we receive personal data because of a data portability request?

When you receive personal data that has been transmitted as part of a data portability request, you need to process this data in line with data protection requirements.

In deciding whether to accept and retain personal data, you should consider whether the data is relevant and not excessive in relation to the purposes for which you will process it. You also need to consider whether the data contains any third party information.

As a new controller, you need to ensure that you have an appropriate lawful basis for processing any third party data and that this processing does not adversely affect the rights and freedoms of those third parties. If you have received personal data which you have no reason to keep, you should delete it as soon as possible. When you accept and retain data, it becomes your responsibility to ensure that you comply with the requirements of the UK GDPR.

In particular, if you receive third party data you should not use this for your own purposes. You should keep the third party data under the sole control of the individual who has made the portability request, and only used for their own purposes.

Example

An individual enters into a contract with a controller for the provision of a service. The controller relies on Article 6(1)(b) to process the individual's personal data. The controller receives information from a data portability request that includes information about third parties. The controller has a legitimate interest to process the third party data under Article 6(1)(f) so that it can provide this service to the individual. However, it should not then use this data to send direct marketing to the third parties.

When can we refuse to comply with a request for data portability?

If an exemption applies, you can refuse to comply with a request for data portability (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information, please see our guidance on [Exemptions](#).

You can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

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

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right to data portability. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
 - 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 sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word “manifestly” means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

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?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- makes a request about the same issue. 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;
- makes an overlapping request, if it relates to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

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

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- 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.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The UK GDPR does not specify how individuals should make data portability requests. Therefore, requests could be made verbally or in writing. They can also be made to any part of your organisation and do not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for data portability' or a reference to 'Article 20 of the UK GDPR', as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, 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 about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

In practice, you may already have processes in place to enable your staff to recognise subject access requests, such as training or established procedures. You could consider adapting them to ensure your staff also recognise data portability requests.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a request for data portability.

However, you can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive. You should base the reasonable fee on the administrative costs of complying with the request.

If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request.

How long do we have to comply?

You must comply with a request for data portability without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:

- any information requested to confirm the requester's identity (see [Can we ask an individual for ID?](#)); or
- a fee (only in certain circumstances – see [Can we charge a fee?](#))

You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

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 have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

Right to restrict processing

At a glance

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Checklists

Preparing for requests for restriction

- We know how to recognise a request for restriction and we understand when the right applies.
- We have a policy in place for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for restriction

- We have processes in place to ensure that we respond to a request for restriction without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We have appropriate methods in place to restrict the processing of personal data on our systems.
- We have appropriate methods in place to indicate on our systems that further processing has been restricted.
- We understand the circumstances when we can process personal data that has been restricted.
- We have procedures in place to inform any recipients if we restrict any data we have shared with them.
- We understand that we need to tell individuals before we lift a restriction on processing.

In brief

- What is the right to restrict processing?
- When does the right to restrict processing apply?
- How do we restrict processing?
- Can we do anything with restricted data?
- Do we have to tell other organisations about the restriction of personal data?
- When can we lift the restriction?
- Can we refuse to comply with a request for restriction?
- What does manifestly unfounded mean?
- What does excessive mean?
- What should we do if we refuse to comply with a request for restriction?
- How do we recognise a request?
- Can we charge a fee?
- How long do we have to comply?
- Can we extend the time for a response?
- Can we ask an individual for ID?

What is the right to restrict processing?

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

When does the right to restrict processing apply?

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

Although this is distinct from the right to rectification and the right to object, there are close links between

those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

How do we restrict processing?

You need to have processes in place that enable you to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

The UK GDPR suggests a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that you consider how you store personal data that you no longer need to process but the individual has requested you restrict (effectively requesting that you do not erase the data).

If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You should also note on your system that the processing of this data has been restricted.

Can we do anything with restricted data?

You must not process the restricted data in any way **except to store it** unless:

- you have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Do we have to tell other organisations about the restriction of personal data?

Yes. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The UK GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who,

under the direct authority of the controller or processor, are authorised to process personal data.

When can we lift the restriction?

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and you are investigating this; or
- the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction.

If you do this, you must inform the individual **before** you lift the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if you are informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that your legitimate grounds override theirs) you should also inform them of the reasons for your refusal to act upon their rights under Articles 16 or 21. You will also need to inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy.

Can we refuse to comply with a request for restriction?

If an exemption applies, you can refuse to comply with a request for restriction (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information, please see our guidance on [Exemptions](#).

You can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

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

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right to restriction. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other

than to cause disruption. For example:

- 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 sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

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?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- makes a request about the same issue. 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;
- makes an overlapping request, if it relates to a completely separate set of information; or

- previously submitted requests which have been manifestly unfounded or excessive.

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

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- 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.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The UK GDPR does not specify how to make a valid request. Therefore, an individual can make a request for restriction verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for restriction' or Article 18 of the UK GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, 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 about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a request for restriction.

However, you can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive. You should base the reasonable fee on the administrative costs of complying with the request.

If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request.

How long do we have to comply?

You must comply with a request for restriction without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:

- any information requested to confirm the requester's identity (see [Can we ask an individual for ID?](#)); or
- a fee (only in certain circumstances – see [Can we charge a fee?](#))

You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

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 have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and

what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 18, 19 and Recital 67 

External link

Further reading – ICO guidance

The [Accountability Framework](#) looks at the ICO's expectations in relation to right to restrict processing.

Right to erasure

At a glance

- The UK GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- The right is not absolute and only applies in certain circumstances.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- This right is not the only way in which the UK GDPR places an obligation on you to consider whether to delete personal data.

Checklists

Preparing for requests for erasure

- We know how to recognise a request for erasure and we understand when the right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure

- We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.
- We have procedures in place to inform any recipients if we erase any data we have shared with them.
- We have appropriate methods in place to erase information.

In brief

- [What is the right to erasure?](#)
- [When does the right to erasure apply?](#)

- How does the right to erasure apply to data collected from children?
- Do we have to tell other organisations about the erasure of personal data?
- Do we have to erase personal data from backup systems?
- When does the right to erasure not apply?
- Can we refuse to comply with a request for other reasons?
- What does manifestly unfounded mean?
- What does excessive mean?
- What should we do if we refuse to comply with a request for erasure?
- How do we recognise a request?
- Can we charge a fee?
- How long do we have to comply?
- Can we extend the time for a response?
- Can we ask an individual for ID?

What is the right to erasure?

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.

The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

How does the right to erasure apply to data collected from children?

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments,

under the UK GDPR.

Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

For further details about the right to erasure and children's personal data please read our guidance on [children's privacy](#).

Do we have to tell other organisations about the erasure of personal data?

The UK GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

The UK GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

Do we have to erase personal data from backup systems?

If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in the context of its backups), and the technical mechanisms that are available to you.

You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. You must ensure that you do not use the data within the backup for any other purpose, ie that the backup is simply held on your systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk,

although this will be context specific. For more information on what we mean by 'putting data beyond use' see our old guidance under the 1998 Act on [deleting personal data](#) (this will be updated in due course).

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

If you are required by law to process individuals' personal data, then the right to erasure will not apply.

The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

For more information about special categories of data please see our [Guide to the UK GDPR](#).

Example

An individual who previously worked for an organisation and has now left asks their old employer to erase all their personal data.

The organisation needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The organisation can refuse the request to erase the individual's data, as they remain under a legal obligation to process it.

Example

A healthcare provider receives a request from a previous patient to erase all of their personal data.

However, the provider's liability insurance requires them to retain patient records in case of complaints or legal claims.

The organisation can refuse the request to erase the individual's data, as they are processing the data for the establishment, exercise or defence of legal claims.

Can we refuse to comply with a request for other reasons?

If an exemption applies, you can refuse to comply with a request for erasure (wholly or partly). Not all of the exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information, please see our guidance on [Exemptions](#).

You can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

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

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right to erasure. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
 - 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 sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously

submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word “manifestly” means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

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?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will **not necessarily** be excessive just because the individual:

- makes a request about the same issue. 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;
- makes an overlapping request, if it relates to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

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

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- 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.

You should also provide this information if you request a reasonable fee or need additional information to

identify the individual.

How do we recognise a request?

The UK GDPR does not specify how to make a valid request. Therefore, an individual can make a request for erasure verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for erasure' or Article 17 of the UK GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, 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 about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a request for erasure.

However, you can charge a "reasonable fee" for the administrative costs of complying with the request if it is manifestly unfounded or excessive. You should base the reasonable fee on the administrative costs of complying with the request.

If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request.

How long do we have to comply?

You must respond to a request for erasure without undue delay and at the latest within one month, letting the individual know whether you have erased the data in question, or that you have refused their request.

The time limit to respond starts on receipt of the request or (if later) on receipt of:

- any information requested to confirm the requester's identity (see [Can we ask an individual for ID?](#)); or
- a fee (only in certain circumstances – see [Can we charge a fee?](#))

You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

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 have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further reading

Right to rectification

At a glance

- The UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the UK GDPR (Article (5)(1)(d)).

Checklists

Preparing for requests for rectification

- We know how to recognise a request for rectification and we understand when this right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for rectification

- We have processes in place to ensure that we respond to a request for rectification without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We have appropriate systems to rectify or complete information, or provide a supplementary statement.
- We have procedures in place to inform any recipients if we rectify any data we have shared with them.

In brief

- [What is the right to rectification?](#)
- [What do we need to do?](#)
- [When is data inaccurate?](#)

- What should we do about data that records a mistake?
- What should we do about data that records a disputed opinion?
- What should we do while we are considering the accuracy?
- What should we do if we are satisfied that the data is accurate?
- Can we refuse to comply with the request for rectification for other reasons?
- What does manifestly unfounded mean?
- What does excessive mean?
- What should we do if we refuse to comply with a request for rectification?
- How can we recognise a request?
- Can we charge a fee?
- How long do we have to comply?
- Can we extend the time for a response?
- Can we ask an individual for ID?
- Do we have to tell other organisations if we rectify personal data?

What is the right to rectification?

Under Article 16 of the UK GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the UK GDPR (Article 5(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

When is data inaccurate?

The UK GDPR does not give a definition of the term accuracy. However, the Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

What should we do about data that records a mistake?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individual's data.

Example

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified.

What should we do about data that records a disputed opinion?

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

What should we do while we are considering the accuracy?

Under Article 18 an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and you are checking it. As a matter of good practice, you should restrict the processing of the personal data in question whilst you are verifying its accuracy, whether or not the individual has exercised their right to restriction. For more information, see our [guidance on the right to restriction](#).

What should we do if we are satisfied that the data is accurate?

You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

Can we refuse to comply with the request for rectification for other reasons?

If an exemption applies, you can refuse to comply with an objection (wholly or partly). Not all of the

exemptions apply in the same way, and you should look at each exemption carefully to see how it applies to a particular request. For more information, please see our guidance on [Exemptions](#).

You can also refuse to comply with a request if it is:

- manifestly unfounded; or
- excessive.

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

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

What does manifestly unfounded mean?

A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right to rectification. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
 - 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 sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. You must consider a request in the context in which it is made, and you are responsible for demonstrating that it is manifestly unfounded.

Also, you should not presume that a request is manifestly unfounded because the individual has previously submitted requests which have been manifestly unfounded or excessive or if it includes aggressive or abusive language.

The inclusion of the word “manifestly” means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

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?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

However, it depends on the particular circumstances. It will not necessarily be excessive just because the individual:

- makes a request about the same issue. 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;
- makes an overlapping request, if it relates to a completely separate set of information; or
- previously submitted requests which have been manifestly unfounded or excessive.

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

You must inform the individual without undue delay and within one month of receipt of the request about:

- the reasons you are not taking action;
- 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.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How can we recognise a request?

The UK GDPR does not specify how to make a valid request. Therefore, an individual can make a request for rectification verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the UK GDPR to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Article 16.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need

specific training to identify a request.

Additionally, 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 about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a request for rectification.

However, you can charge a “reasonable fee” for the administrative costs of complying with the request if it is manifestly unfounded or excessive. You should base the reasonable fee on the administrative costs of complying with the request.

If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

Alternatively, you can refuse to comply with a manifestly unfounded or excessive request.

How long do we have to comply?

You must comply with a request for rectification without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of:

- any information requested to confirm the requester’s identity (see [Can we ask an individual for ID?](#)); or
- a fee (only in certain circumstances – see [Can we charge a fee?](#))

You should calculate the time limit from the day you receive the request (whether it is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the same day. This gives the organisation until 3 October to comply with the request.

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 have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Do we have to tell other organisations if we rectify personal data?

If you have disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The UK GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5, 12, 16 and 19 

External link

Right of access

In more detail – ICO guidance

We have produced more [detailed guidance on the right of access](#).

At a glance

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- This is commonly referred to as a subject access request or 'SAR'.
- Individuals can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- In most circumstances, you cannot charge a fee to deal with a request.
- You should respond without delay and within one month of receipt of the request.
- You may extend the time limit by a further two months if the request is complex or if you receive a number of requests from the individual.
- You should perform a reasonable search for the requested information.
- You should provide the information in an accessible, concise and intelligible format.
- The information should be disclosed securely.
- You can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

Checklists

Preparing for subject access requests

- We know how to recognise a subject access request and we understand when the right of access applies.
- We have a policy for how to record requests we receive verbally.
- We understand what steps we need to take to verify the identity of the requester, if necessary.
- We understand when we can pause the time limit for responding if we need to ask for clarification.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- We understand the nature of the supplementary information we need to provide in response to a subject access request.

- We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Complying with subject access requests

- We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.
- We understand how to perform a reasonable search for the information.
- We understand what we need to consider if a third party makes a request on behalf of an individual.
- We are aware of the circumstances in which we can extend the time limit to respond to a request.
- We understand how to assess whether a child is mature enough to understand their rights.
- We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
- We understand what we need to consider if a request includes information about others.
- We are able to deliver the information securely to an individual, and in the correct format.

In brief

- [What is the right of access?](#)
- [How do we recognise a subject access request \(SAR\)?](#)
- [What about requests for information about children?](#)
- [What should we consider when responding to a request?](#)
- [Can we ask for ID?](#)
- [Can we charge a fee?](#)
- [How do we find and retrieve the relevant information?](#)
- [How should we supply information to the requester?](#)
- [When can we refuse to comply with a request?](#)
- [What should we do if the request involves information about other individuals?](#)
- [What other exemptions are there?](#)
- [Are there any special cases?](#)
- [Can the right of access be enforced?](#)
- [Can we force an individual to make a SAR?](#)

What is the right of access?

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

How do we recognise a subject access request (SAR)?

An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

An individual may ask a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. You may also receive a SAR made on behalf of an individual through an online portal. Before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

What about requests for information about children?

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the request is from a child and you are confident they can understand their rights, you should usually respond directly to the child. You may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

What should we consider when responding to a request?

You must comply with a SAR without undue delay and at the latest within one month of receiving the request. You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual, eg other types of requests relating to individuals' rights.

If you process a large amount of information about an individual, you may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until you receive clarification, although you should supply any of the supplementary information you can do within one month.

Can we ask for ID?

Yes. You need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to a SAR does not begin until you have received the requested information. However, you should request ID documents promptly.

Can we charge a fee?

Not usually. In most cases you cannot charge a fee to comply with a SAR. However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

How do we find and retrieve the relevant information?

You should make reasonable efforts to find and retrieve the requested information. However, you are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

How should we supply information to the requester?

An individual is entitled to a copy of their personal data and to other supplementary information (which largely corresponds with the information that you should provide in a privacy notice). If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

When deciding what format to use, you should consider both the circumstances of the particular request and whether the individual has the ability to access the data you provide in that format. It is good practice to establish the individual's preferred format prior to fulfilling their request. Alternatives can also include allowing the individual to access their data remotely and download a copy in an appropriate format.

If an individual asks, you can provide a verbal response to their SAR, provided that you have confirmed their identity by other means. You should keep a record of the date they made the request, the date you responded, details of who provided the information and what information you provided.

As the controller of the information you are responsible for taking all reasonable steps to ensure its security. Please see our detailed guidance '[How do we provide the information securely?](#)' for more information.

When can we refuse to comply with a request?

Where an exemption applies, you may refuse to provide all or some of the requested information, depending on the circumstances. You can also refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive. [Our detailed guidance](#) explains the factors you should consider in determining whether a request is manifestly unfounded or excessive.

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

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

What should we do if the request involves information about other individuals?

Where possible, you should consider whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, you do not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

[Our detailed guidance](#) provides further information on what you need to consider in these circumstances.

You need to respond to the requester whether or not you decide to disclose information about a third party.

You must be able to justify your decision to disclose or withhold information about a third party, so you should keep a record of what you decide and why.

What other exemptions are there?

The exemptions are set out in Schedules 2 and 3 of the DPA 2018 and they are as follows:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions

[Our detailed guidance](#) explains how each of these exemptions work in practice. While the exemptions listed above are those most likely to apply in practice, the DPA 2018 contains additional exemptions that may be relevant when dealing with a SAR. For more information, please see our [guidance about exemptions](#).

Are there any special cases?

Yes. There are special rules and provisions about SARs and some categories of personal data, including:

- unstructured manual records;
- credit files;
- health data;
- educational data; and
- social work data.

[Our detailed guidance](#) provides further details of these special rules and provisions.

Can the right of access be enforced?

Yes. In appropriate cases, the ICO may take action against a controller or processor if they fail to comply with data protection legislation. The ICO will exercise these enforcement powers in accordance with our Regulatory Action Policy.

If you fail to comply with a SAR, the requester may apply for a court order requiring you to comply or to seek compensation. It is a matter for the court to decide, in each particular case, what action to take.

Can we force an individual to make a SAR?

No. An enforced SAR is when someone requires an individual to make a SAR to gain access to certain information about them (eg their convictions, cautions or health records). This information is then used, for example, as supporting evidence regarding a job application or before entering into a contract for insurance. Forcing an individual to make a SAR in such circumstances is a criminal offence.

You should consult our [detailed guidance](#) for further detail about the circumstances in which it is unlawful to require an individual to make a SAR.

Further Reading

 Relevant provisions in the legislation See UK GDPR Articles 12, 15 and Recitals 59, 63 
External link

Further reading – ICO guidance

The [Accountability Framework](#) looks at the ICO's expectations in relation to right of access.

[Responses to the consultation on the draft right of access detailed guidance](#)

[ICO's consultation: a summary of responses](#)

Right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- 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'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklists

What to provide

We provide individuals with all the following privacy information:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.

- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

- We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month;
- if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

- concise;
- transparent;
- intelligible;

- easily accessible; and
- uses clear and plain language.

Changes to the information

- We regularly review and, where necessary, update our privacy information.
- If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

- We undertake an information audit to find out what personal data we hold and what we do with it.
- We put ourselves in the position of the people we're collecting information about.
- We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

In brief

- [What is the right to be informed and why is it important?](#)
- [What privacy information should we provide?](#)
- [When should we provide privacy information?](#)
- [Are there any exceptions?](#)
- [How should we draft our privacy information?](#)
- [What methods can we use to provide privacy information?](#)
- [What common issues might come up in practice?](#)
- [The right to be informed in more detail](#)

What is the right to be informed and why is it important?

The right to be informed covers some of the key transparency requirements of the UK GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.

Articles 13 and 14 of the UK GDPR specify what individuals have the right to be informed about. We call this 'privacy information'.

Using an effective approach can help you to comply with other aspects of the UK GDPR, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to fines and lead to reputational damage.

What privacy information should we provide?

The table below summarises the information that you must provide. What you need to tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓

The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

When should we provide privacy information?

When you collect personal data from the individual it relates to, you must provide them with privacy information at the time you obtain their data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month;
- if you use the data to communicate with the individual, at the latest, when the first communication takes place; or
- if you envisage disclosure to someone else, at the latest, when you disclose the data.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

Are there any exceptions?

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

When obtaining personal data from other sources, you do not need to provide individuals with privacy information if:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

How should we draft our privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalised, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

What methods can we use to provide privacy information?

There are a number of techniques you can use to provide people with privacy information. You can use:

- **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.

What common issues might come up in practice?

If you **share** personal data with (or **sell** it to) other organisations:

- As part of the privacy information you provide, you must tell people who you are giving their information to, unless you are relying on an exception or an exemption.
- You can tell people the names of the organisations or the categories that they fall within; choose the option that is most meaningful.
- It is good practice to use a dashboard to let people manage who their data is sold to, or shared with, where they have a choice.

If you **buy** personal data from other organisations:

- You must provide people with your own privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, or it would involve a disproportionate effort, you must carry out a DPIA to find ways to mitigate the risks of the processing.
- If your purpose for using the personal data is different to that for which it was originally obtained, you must tell people about this, as well as what your lawful basis is for the processing.
- Provide people with your privacy information within a reasonable period of buying the data, and no later than one month.

If you obtain personal data from **publicly accessible sources**:

- You still have to provide people with privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, or it would involve a disproportionate effort, you must carry out a DPIA to find ways to mitigate the risks of the processing.
- Be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from a number of different sources.
- Provide people with privacy information within a reasonable period of obtaining the data, and no later than one month.

If you apply **Artificial Intelligence (AI)** to personal data:

- Be upfront about it and explain your purposes for using AI.
- If the purposes for processing are unclear at the outset, give people an indication of what you are going to do with their data. As your processing purposes become clearer, update your privacy information and actively communicate this to people.
- Inform people about any new uses of personal data before you actually start the processing.
- If you use AI to make solely automated decisions about people with legal or similarly significant effects, tell them what information you use, why it is relevant and what the likely impact is going to be.
- Consider using just-in-time notices and dashboards which can help to keep people informed and let them control further uses of their personal data.

Accountability and governance

At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the UK GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must, take including:
 - adopting and implementing data protection policies;
 - taking a 'data protection by design and default' approach;
 - putting written contracts in place with organisations that process personal data on your behalf;
 - maintaining documentation of your processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer; and
 - adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

Checklist

We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.

We keep evidence of the steps we take to comply with the UK GDPR.

We put in place appropriate technical and organisational measures, such as:

- adopting and implementing data protection policies (where proportionate);
- taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- putting written contracts in place with organisations that process personal data on our

behalf;

- maintaining documentation of our processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer (where necessary); and
 - adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- We review and update our accountability measures at appropriate intervals.

In brief

- [What is accountability?](#)
- [Why is accountability important?](#)
- [What do we need to do?](#)
- [Should we implement data protection policies?](#)
- [Should we adopt a 'data protection by design and default' approach?](#)
- [Do we need to use contracts?](#)
- [What documentation should we maintain?](#)
- [What security measures should we put in place?](#)
- [How do we record and report personal data breaches?](#)
- [Should we carry out data protection impact assessments \(DPIAs\)?](#)
- [Should we assign a data protection officer \(DPO\)?](#)
- [Should we adhere to codes of conduct and certification schemes?](#)
- [What else should we consider?](#)

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 5 and 24, and Recitals 39 and 74](#) 
External link

What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are **responsible** for complying with the GDPR. Second, you must be able to **demonstrate** your compliance.

Article 5(2) of the GDPR says:

“

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Further Reading

 Relevant provisions in the UK GDPR - See Article 5 and Recitals 39 and 74 

External link

Further reading – ICO guidance

Principles

Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

Further Reading

 Relevant provisions in the UK GDPR - See Article 83 

External link

What do we need to do?

Accountability is not a box-ticking exercise. Being **responsible** for compliance with the UK GDPR means that you need to be proactive and organised about your approach to data protection, while **demonstrating** your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the UK GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Article 24(1) of the UK GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the UK GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The UK GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for instance, you handle large volumes of personal data, or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake ([see below for more on data protection officers](#)).

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 24\(2\) and Recital 78](#) 

External link

Relevant provisions in the UK GDPR - See Recital 78

External link

Should we adopt a ‘data protection by design and default’ approach?

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading ‘data protection by design and by default’, the UK GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The UK GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in [data protection impact assessments – see below](#)) demonstrates this.

Further reading

Relevant provisions in the UK GDPR - See Article 25

External link

Relevant provisions in the UK GDPR - See Recital 78

External link

Further reading – ICO guidance

[Data protection by design and default](#)

[Anonymisation code of practice](#)

Do we need to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party’s responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

Further Reading

Relevant provisions in the UK GDPR - See Article 28

External link

Relevant provisions in the UK GDPR - See Recital 81

External link

Further reading – ICO guidance

Contracts

What documentation should we maintain?

Under Article 30 of the UK GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a great way to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the UK GDPR such as making sure that the information you hold about people is accurate and secure.

As well as your record of processing activities under Article 30, you also need to document other things to show your compliance with the UK GDPR. For instance, you need to keep records of consent and any personal data breaches.

Further Reading

Relevant provisions in the UK GDPR - See Articles 7(1), 30 and 33(5), and Recitals 42 and 82

External link

Further reading – ICO guidance

Documentation

Consent

Personal data breaches

What security measures should we put in place?

The UK GDPR repeats the requirement to implement technical and organisational measures to comply with the UK GDPR in the context of security. It says that these measures should ensure a level of security appropriate to the risk.

You need to implement security measures if you are handling any type of personal data, but what you put

in place depends on your particular circumstances. You need to ensure the confidentiality, integrity and availability of the systems and services you use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5(f) and 32, and Recitals 39 and 83 
External link

Further reading – ICO guidance

Security

How do we record and report personal data breaches?

You must report certain types of personal data breach to the Information Commissioner's Office (ICO), and in some circumstances, to the affected individuals as well.

Additionally, the UK GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 33-34 and Recitals 85-88 
External link

Further reading – ICO guidance

Personal data breaches

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

WP29 adopted guidelines on [Personal data breach notification](#), which have been adopted by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Should we carry out data protection impact assessments (DPIAs)?

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the UK GDPR, while also acting as documented evidence of your decision-making and the steps you took.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 35-36, and Recitals 84 and 89-95](#) 

External link

Further reading – ICO guidance

[Data protection impact assessments](#)

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted guidelines on [data protection impact assessments](#), which have been endorsed by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues".

Should we assign a data protection officer (DPO)?

Some organisations are required to appoint a DPO. A DPO's tasks include advising you about the UK GDPR, monitoring compliance and training staff.

Your DPO must report to your highest level of management, operate independently, and have adequate

resources to carry out their tasks.

Even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the UK GDPR.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 37-39](#) 

External link

 [Relevant provisions in the UK GDPR - Recital 97](#) 

External link

Further reading – ICO guidance

[Data protection officers](#)

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted guidelines on [data protection officers](#), which have been endorsed by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues".

Should we adhere to codes of conduct and certification schemes?

Under the UK GDPR, trade associations and representative bodies may draw up codes of conduct covering topics such as fair and transparent processing, pseudonymisation, and the exercise of people's rights.

In addition, the ICO or accredited certification bodies can issue certification of the data protection compliance of products and services.

Both codes of conduct and certification are voluntary, but they are an excellent way of verifying and demonstrating that you comply with the GDPR.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 40-43, and Recitals 98 and 100](#) 

Further reading – ICO guidance

[Codes of conduct and certification](#)

What else should we consider?

The above measures can help to support an accountable approach to data protection, but it is not limited to these. You need to be able to prove what steps you have taken to comply. In practice this means keeping records of what you do and justifying your decisions.

Example

A company wants to use the personal data it holds for a new purpose. It carries out an assessment in line with Article 6(4) of the UK GDPR, and determines that the new purpose is compatible with the original purpose for which it collected the personal data. Although this provision of the UK GDPR does not specify that the company must document its compatibility assessment, it knows that to be accountable, it needs to be able to prove that their handling of personal data is compliant with the UK GDPR. The company therefore keeps a record of the compatibility assessment, including its rationale for the decision and the appropriate safeguards it put in place.

Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as ‘accountable’ and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 12-14, 22 and 24\(1\), and Recitals 39, 58-61 and 71](#) 

Data protection fee

On 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 (the 2018 Regulations) came into force, changing the way we fund our data protection work.

Under the 2018 Regulations, organisations that determine the purpose for which personal data is processed (controllers) must pay a data protection fee unless they are exempt.

The new data protection fee replaces the requirement to 'notify' (or register), which was in the Data Protection Act 1998 (the 1998 Act).

Although the 2018 Regulations come into effect on 25 May 2018, this doesn't mean everyone now has to pay the new fee. Controllers who have a current registration (or notification) under the 1998 Act do not have to pay the new fee until that registration has expired.

From 1 April 2019, the Data Protection (Charges and Information) (Amendment) Regulations 2019 exempted the processing of personal data by members of the House of Lords, elected representatives and prospective representatives.

'Elected representatives' is defined by the Data Protection Act 2018 and includes, but is not limited to, MPs, MSPs, AMs in Wales, MEPs, elected councillors in county councils, district councils, London boroughs, parish councils, elected mayors and police and crime commissioners.

'Prospective representative' refers to anyone seeking to become an elected representative as defined above.

[Find out more about paying the data protection fee here.](#)

Certification

Certification is a way for an organisation to demonstrate compliance with UK GDPR. Certification scheme criteria will be approved by the ICO and can cover a specific issue or be more general. Once an accredited certification body has assessed and approved an organisation, it will issue them with a certificate, and a seal or mark relevant to that scheme.

At a glance

- Certification is a way to demonstrate your compliance with the UK GDPR and enhance transparency.
- Certification criteria should reflect the needs of small and medium sized enterprises.
- Certification criteria are approved by the ICO and certification issued by accredited certification bodies.
- Certification will be issued to data controllers and data processors in relation to specific processing activities.
- Applying for certification is voluntary. However, if there is an approved certification scheme that covers your processing activity, you may wish to consider having your processing activities certified as it can help you demonstrate compliance to the regulator, the public and in your business to business relationships.

In brief

- [What is the purpose of certification?](#)
- [Who is responsible for certification?](#)
- [What can be certified?](#)
- [What must certification scheme criteria contain?](#)
- [Why should we apply for certification of our processing?](#)
- [What are the practical implications for us?](#)
- [What happens next?](#)
- [Frequently asked questions](#)
- [In detail](#)
- [Certification scheme register](#)

What is the purpose of certification?

Certification is a way of demonstrating that your processing of personal data complies with the UK GDPR requirements, in line with the accountability principle. Certification can help demonstrate data protection in a practical way to businesses, individuals and regulators. Your customers can use certification as a means to quickly assess the level of data protection of your particular product, process or service, which provides transparency both for data subjects and in business to business relationships.

The UK GDPR says that certification is also a means to:

- demonstrate compliance with the provisions on data protection by design and by default (Article 25(3));
- demonstrate that you have appropriate technical and organisational measures to ensure data security (Article 32(3)); and
- to support transfers of personal data to third countries or international organisations (Article 46(2)(f)).

Who is responsible for certification?

The ICO encourages the use of data protection certification mechanisms as a means to enhance transparency and compliance with the UK GDPR.

The certification framework involves:

- us publishing accreditation requirements for certification bodies to meet;
- the UK's national accreditation body, UKAS, accrediting certification bodies and maintaining a public register;
- us approving and publishing certification criteria;
- accredited certification bodies issuing certification against those criteria;
- controllers and processors applying for certification and using it to demonstrate compliance; and
- the ICO maintaining a public register of approved certification schemes.

What can be certified?

The scope of a certification scheme could be quite general and be applied to a variety of different products, processes or services; or it could be specific, for example, secure storage and protection of personal data contained within a digital vault.

Certification will relate to specific personal data processing operations that take place in a product, process or service offered by a controller or processor. Those processing operations will be assessed against the certification criteria by the accredited certification body.

Certification can only be issued to data controllers and processors and cannot therefore be used to certify individuals, for example data protection officers.

Article 42(2) also allows for the use of certification schemes for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to UK GDPR for international transfers of personal data.

What must certification scheme criteria contain?

Certification criteria must be:

- derived from UK GDPR principles and rules, as relevant to the scope of certification, ie:
 - lawfulness of processing (Art 6-10)
 - principles of data processing (Art 5)
 - data subjects' rights (Art 12-23)
 - obligation to notify data breaches (Art 33)

- obligation of DP by design and default (Art 25)
- whether a DPIA has been completed where required (Art35(7)(d))
- technical and organisational measures put in place to ensure security (Art 32);
- formulated in such a way that they are clear and allow practical application;
- auditable (ie specify objectives and how they can be achieved so as to demonstrate compliance);
- relevant to the target audience;
- inter-operable with other standards, for example ISO standards; and
- scalable for application to different size or type of organisations.

These conditions are outlined in full in our [detailed guidance](#).

Once your organisation has been successfully assessed by the accredited certification body, you will be issued with a data protection certificate, seal or mark relevant to that scheme.

Why should we apply for certification of our processing?

Applying for certification is voluntary. However, if there is an approved certification scheme that covers your processing activity, you may wish to consider working towards it as a way of demonstrating that you comply with the UK GDPR.

Certification provides a framework for you to follow, thereby helping ensure compliance and offering assurance that specific standards are being adhered to, for example in a processor to controller relationship.

Obtaining certification for your processing can also help you to:

- be more transparent and accountable - enabling businesses or individuals to distinguish which processing activities, operations and services meet UK GDPR data protection requirements and they can trust with their personal data;
- have a competitive advantage;
- create effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals;
- improve standards by establishing best practice;
- help with international transfers; and
- mitigate against enforcement action.

What are the practical implications for us?

- As a controller or processor, you could obtain certification for your processing operations within your products, processes and services. Certification bodies will use independent assessors, giving an independent expert view on whether you meet the certification criteria. You will need to provide them with all the necessary information and access to your processing activities to enable them to conduct the certification procedure.
- Certification is valid for a maximum of three years, subject to periodic reviews. These independent reviews provide assurance that the certification can be trusted. However, certifications can be withdrawn

- if you no longer meet the certification criteria, and the certification body will notify us of this.
- Your customers can view your certification in a public register of certificates published by certification bodies.
 - Certification can help you demonstrate compliance but does not reduce your wider data protection responsibilities outside the certified processing activity.
 - When contracting work to third parties, you may wish to consider whether they hold a UK GDPR certificate for their processing operations, as part of meeting your due diligence requirements under the UK GDPR.

What happens next?

You can find details of approved certification schemes in the [register of certification criteria](#). If there is a scheme that meets your needs, you should contact the relevant certification body who is accredited to operate the scheme.

We have published further information about [how to apply for UK GDPR certification](#) in our detailed guidance.

Frequently asked questions

We have published [answers to frequently asked questions](#) relating to certification schemes.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 42-43 and 83 and Recitals 81 and 100](#)
External link

In detail

We have published [detailed guidance on certification](#).

In more detail - European Data Protection Board

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Certification Guidelines and Annex

The EDPB published adopted '[Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation](#)' on 4 June 2019.

Codes of conduct

Under the UK GDPR, trade associations and other representative bodies may draw up codes of conduct that identify and address data protection issues that are important to their members, such as fair and transparent processing, pseudonymisation or the exercise of people's rights. They are a good way of developing sector-specific guidelines to help with compliance with the UK GDPR. There is a real benefit to developing a code of conduct as it can help to build public trust and confidence in your sector's ability to comply with data protection laws.

The ICO is committed to encouraging the development of codes of conduct and will provide advice and support from the start on:

- meeting the necessary criteria;
- the requirements of the UK GDPR; and
- complex areas of data protection.

We welcome informal discussions with organisations as part of your development of your code of conduct and prior to formal submission. Please read our [detailed guidance pages](#) for further information.

At a glance

- Codes of conduct enable a sector to own and resolve key data protection challenges. The ICO see these as a way of demonstrating accountability and encourage trade associations and bodies who are able to speak on behalf of a group of organisations, to create codes of conduct.
- Using an ICO approved code of conduct give assurance that the code and its monitoring is appropriate and will help you to apply the UK GDPR effectively.
- Codes of conduct should reflect the requirements of different processing sectors and takes account of the specific needs of small and medium sized enterprises.
- Trade associations or bodies who are able to speak on behalf of a group of organisations can create, amend or extend codes of conduct to help their sector comply with the UK GDPR in a practical, transparent and cost-effective way.
- Signing up to a code of conduct is voluntary. However, if there is an approved code of conduct, relevant to your processing, you should consider signing up.
- A code of conduct can help you to reflect on your processing activities and ensure you follow rules designed for your sector to achieve best practice.
- A draft code of conduct must be submitted to us for approval and will be assessed against specific criteria to ensure that it meets the expected standard.
- A code of conduct will describe the appropriate monitoring mechanisms and (where applicable) the monitoring bodies that will be accredited to monitor compliance as part of the code approval process.

In brief

Codes of conduct help you to apply the UK GDPR effectively and allow you to demonstrate your compliance.

- What are codes of conduct?
- Why sign up to a code of conduct?
- What should a code of conduct address?
- Who is responsible for codes of conduct?
- How will the ICO approve a code of conduct?
- How will compliance with the code be monitored?
- How to become a monitoring body
- How can we demonstrate independence for an internal monitoring body?
- What are the practical implications for our organisation?
- How do we sign up to become a code member?
- Next steps
- In detail

What are codes of conduct?

Codes of conduct are voluntary accountability tools, enabling sectors to identify and resolve key data protection challenges in their sector with assurance from ICO that the code, and its monitoring, is appropriate. They can help you to reflect on your processing activities and ensure you follow rules designed for your sector to achieve good practice. They are written by an organisation or association representing a sector in a way that the sector understands and enable sectors to solve these challenges with advice and support from the ICO.

By signing up to a code of conduct, controllers and processors can ensure they apply the UK GDPR effectively and in doing so establish operational norms in compliance that ultimately should assist in bringing down levels of non-compliance. Codes of conduct require a monitoring method, and for private or non-public authorities, a monitoring body to deliver them.

Why sign up to a code of conduct?

Adhering to a code of conduct shows that you:

- follow UK GDPR requirements for data protection that have been agreed as good practice within your sector; and
- are appropriately addressing the type of processing you are doing and the related level of risk. For example, a code may contain specific sectoral requirements when it relates to processing of sensitive special category personal data.

Adhering to a code of conduct could help you to:

- be more transparent and accountable;
- take into account the specific requirements of processing carried out in a sector and improve standards by following best practice in a cost-effective way;
- promote confidence in a sector by creating effective safeguards to mitigate the risk around processing activities;

- earn the trust and confidence of data subjects and promote the rights and freedoms of individuals;
- help with specific data protection areas, such as breach notification and privacy by design; and
- improve the trust and confidence in your organisation's compliance with UK GDPR and of the general public about what happens to their personal data.

What should a code of conduct address?

Codes of conduct should help you to comply with the UK GDPR, and may cover topics such as fair and transparent processing, legitimate interests, pseudonymisation or alternative, appropriate data protection processing issues.

Codes of conduct should also reflect the specific needs of controllers and processors in small and medium enterprises and help them to work together to apply UK GDPR requirements to specific issues that they face.

Codes should provide added value for their sector, as they will tailor the UK GDPR requirements to the sector or area of data processing. They could be a cost-effective means to enable compliance with the UK GDPR for a sector and its members.

Who is responsible for codes of conduct?

Trade associations or bodies who are able to speak on behalf of controllers or processors can create a code of conduct in consultation with relevant stakeholders, including the public where feasible. They can amend or extend existing codes to comply with UK GDPR requirements. They have to submit the draft code to us for approval.

We encourage the creation of codes of conduct by actively engaging with sectors to encourage development and uptake of codes of conduct where the sector would benefit. We will also support organisations who approach the ICO with a proposal for a code of conduct.

We will:

- Provide advice and guidance to bodies considering or developing a code;
- check that codes meet the code criteria set out below;
- accredit (approve) monitoring bodies;
- approve and publish codes of conduct; and
- maintain a public register of all approved UK codes of conduct.

How will the ICO approve a code of conduct?

All codes of conduct received will be assessed against the following criteria to ensure that the code submission addresses the following:

- Outlines the code owner's ability to represent controllers or processors covered by the code.
- Includes a concise statement explaining the purpose of the code, the benefits to members and how it effectively applies the UK GDPR.
- Identifies processing operations that the code covers and the categories of controllers or processors that

it applies to as well as what the data protection issues are that it intends to address.

- Identifies suitable monitoring methods to assess code member compliance with the code.
- Identifies the monitoring body and its legal status (only required for codes covering non-public authorities).
- Outlines the stakeholder consultation and outcomes.
- Complies with other relevant national legislation, where required.
- Specifies whether it is a national code or a code for use as an international transfer tool.

How will compliance with the code be monitored?

All codes of conduct must contain suitable methods to allow for effective monitoring of code member compliance and outline appropriate action in cases of infringement. In all cases these methods will need to be clear, suitable and efficient.

Codes of conduct covering the private sector, or any non-public bodies will also have to identify a monitoring body to fulfil the code monitoring requirements. Monitoring bodies must be accredited (approved) by the ICO.

How to become a monitoring body

There are a number of requirements that should be met in order for a monitoring body to gain ICO accreditation. Code owners will need to demonstrate as a minimum how their proposed monitoring body:

- Is independent from code owners.
- Can act free from sanctions or external influence to ensure that no conflict of interest arises.
- Has the required knowledge and expertise.
- Has established procedures and sufficient resources for the monitoring of compliance with the code.
- Has an open and transparent complaints handling process.
- Will communicate to the ICO infringements that lead to suspensions or exclusions of code members.
- Will review the code to ensure that the code remains relevant and up to date.
- Has appropriate legal status.

[The ICO accreditation requirements can be found here](#). You can also find out more about monitoring body accreditation on our [detailed guidance pages](#).

How can we demonstrate independence for an internal monitoring body?

A code owner will have to demonstrate how the monitoring body can remain impartial from, code members, the profession, industry or sector to which the code applies.

How this will work in practice will vary depending on the code topic, the sector and the organisations involved so there is no universal approach to demonstrating independence.

Code owners will need to consider the risks to impartiality and demonstrate how they will minimise or remove these risks on an ongoing basis.

We expect that in some cases existing models of self-regulation or co –regulation familiar to representative bodies and trade associations may be adapted to meet these requirements. Existing good practice in these areas could all help to prove impartiality, such as:

- being able to evidence the ability to act free from inappropriate influence;
- separate decision-making arrangements;
- separate staff and governance reporting lines;
- separate funding arrangements or budget management; and
- technical measures, such as information barriers.

What are the practical implications for our organisation?

- You can sign up to a code of conduct relevant to your data processing activities or sector. This could be an extension or an amendment to a current code, or a brand-new code.
- Your customers will be able to view your code membership via the code's webpage and the ICO's public register of UK approved codes of conduct.
- Once you are assessed as adhering to the code, your compliance with the code will be monitored on a regular basis. This monitoring provides assurance that the code can be trusted. Your membership can be withdrawn if you no longer meet the requirements of the code, and the monitoring body will notify us of this.
- When contracting work to third parties, you may wish to consider whether they have signed up to a code of conduct, as part of meeting your due diligence requirements under the UK GDPR.

How do we sign up to become a code member?

The ICO has not yet formally approved any codes of conduct. You may wish to contact your trade association/representative body or a body able to legitimately speak on your behalf to discuss whether they are developing a code in your sector.

For further information please see our [detailed guidance pages](#).

Next steps

We welcome enquiries from organisations who are considering writing, monitoring or signing up to a code of conduct, you can find out more about this on the [detailed guidance pages](#).

In detail

We have published [detailed guidance on codes of conduct](#).

Further Reading

 Relevant provisions in the UK GDPR - See Articles 40-1 and 83 and Recitals 77, 98, 99 and 168
External link

Data protection officers

At a glance

- The UK GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.
- 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's Office (ICO).
- 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.

Checklists

Appointing a DPO

- We are a public authority or body and have appointed a DPO (except if we are a court acting in our judicial capacity).
- We are not a public authority or body, but we know whether the nature of our processing activities requires the appointment of a DPO.
- We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.
- We aren't required to appoint a DPO under the UK GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

Position of the DPO

- Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.
- We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.
- Our DPO is sufficiently well resourced to be able to perform their tasks.
- We do not penalise the DPO for performing their duties.
- We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

- Our DPO is tasked with monitoring compliance with the UK GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
- We will take account of our DPO's advice and the information they provide on our data protection obligations.
- When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.
- Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.
- When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

- Our DPO is easily accessible as a point of contact for our employees, individuals and the ICO.
- We have published the contact details of the DPO and communicated them to the ICO.

In brief

- Do we need to appoint a Data Protection Officer?
- What is the definition of a public authority?
- What are 'core activities'?
- What does 'regular and systematic monitoring of data subjects on a large scale' mean?
- What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?
- What professional qualities should the DPO have?
- What are the tasks of the DPO?
- Can we assign other tasks to the DPO?
- Can the DPO be an existing employee?
- Can we contract out the role of the DPO?
- Can we share a DPO with other organisations?
- Can we have more than one DPO?
- What do we have to do to support the DPO?
- What details do we have to publish about the DPO?
- Is the DPO responsible for compliance?

Do we need to appoint a Data Protection Officer?

Under the UK GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

This applies to both controllers and processors. You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

Regardless of whether the UK GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the UK GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can be seen to play a key role in your organisation's data protection governance structure and to help improve accountability.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle.

Further Reading

Does my organisation need a data protection officer (DPO)?

For organisations

What is the definition of a public authority?

Section 7 of the Data Protection Act 2018 defines what a 'public authority' and a 'public body' are for the purposes of the UK GDPR.

What are 'core activities'?

The other two conditions that require you to appoint a DPO only apply when:

- your core activities consist of processing activities, which, by virtue of their nature, scope and / or their purposes, require the regular and systematic monitoring of individuals on a large scale; or
- your core activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (eg payroll or HR information), but which is not part of carrying out your primary objectives.

Example

For most organisations, processing personal data for HR purposes will be a secondary function to their main business activities and so will not be part of their core activities.

However, a HR service provider necessarily processes personal data as part of its core activities to provide HR functions for its client organisations. At the same time, it will also process HR information for its own employees, which will be regarded as an ancillary function and not part of its core activities.

What does ‘regular and systematic monitoring of data subjects on a large scale’ mean?

There are two key elements to this condition requiring you to appoint a DPO. Although the UK GDPR does not define ‘regular and systematic monitoring’ or ‘large scale’, the Article 29 Working Party (WP29) provided some guidance on these terms in its [guidelines on DPOs](#). WP29 has been replaced by the European Data Protection Board (EDPB) which has endorsed these guidelines. Although these guidelines relate to the EU version of the GDPR, they are also a useful resource for understanding the requirements of the UK GDPR.

‘Regular and systematic’ monitoring of data subjects includes all forms of tracking and profiling, both online and offline. An example of this is for the purposes of behavioural advertising.

When determining if processing is on a large scale, the guidelines say you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example

A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.

What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?

Processing special category data or criminal conviction or offences data carries more risk than other

personal data. So when you process this type of data on a large scale you are required to appoint a DPO, who can provide more oversight. Again, the factors relevant to large-scale processing can include:

- the numbers of data subjects;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the activity.

Example

A health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information. This can be considered as processing special category data on a large scale.

What professional qualities should the DPO have?

- The UK GDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.
- It doesn't specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.
- So, where the processing of personal data is particularly complex or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.
- It would be an advantage for your DPO to also have a good knowledge of your industry or sector, as well as your data protection needs and processing activities.

What are the tasks of the DPO?

The DPO's tasks are defined in Article 39 as:

- to inform and advise you and your employees about your obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and with your data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, [data protection impact assessments](#);
- to cooperate with the ICO; and
- to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

It's important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

Can we assign other tasks to the DPO?

The UK GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Example

As an example of assigning other tasks, Article 30 requires that organisations must maintain records of processing operations. There is nothing preventing this task being allocated to the DPO.

Basically this means the DPO cannot hold a position within your organisation that leads him or her to determine the purposes and the means of the processing of personal data. At the same time, the DPO shouldn't be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

Examples

A company's head of marketing plans an advertising campaign, including which of the company's customers to target, what method of communication and the personal details to use. This person cannot also be the company's DPO, as the decision-making is likely to lead to a conflict of interests between the campaign's aims and the company's data protection obligations.

On the other hand, a public authority could appoint its existing FOI officer / records manager as its DPO. There is no conflict of interests here as these roles are about ensuring information rights compliance, rather than making decisions about the purposes of processing.

Can the DPO be 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 appoint an existing employee as your DPO, rather than you having to create a new post.

Can we contract out the role of the DPO?

You can contract out the role of DPO externally, based on a service contract with an individual or an organisation. It's important to be aware that an externally-appointed DPO should have the same position, tasks and duties as an internally-appointed one.

Can we share a DPO with other organisations?

- You may appoint a single DPO to act for a group of companies or public authorities.
- If your DPO covers several organisations, they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider if one DPO can realistically cover a large or complex collection of organisations. You need to ensure they have the necessary resources to carry out their role and be supported with a team, if this is appropriate.
- Your DPO must be easily accessible, so their contact details should be readily available to your employees, to the ICO, and people whose personal data you process.

Can we have more than one DPO?

- The UK GDPR clearly provides that an organisation must appoint a single DPO to carry out the tasks required in Article 39, but this doesn't prevent it appointing other data protection specialists as part of a team to help support the DPO.
- You need to determine the best way to set up your organisation's DPO function and whether this necessitates a data protection team. However, there must be an individual designated as the DPO for the purposes of the UK GDPR who meets the requirements set out in Articles 37-39.
- If you have a team, you should clearly set out the roles and responsibilities of its members and how it relates to the DPO.
- If you hire data protection specialists other than a DPO, it's important that they are not referred to as your DPO, which is a specific role with particular requirements under the UK GDPR.

What do we have to do to support the DPO?

You must ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, ie board level;
- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- you provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their UK GDPR obligations, and to maintain their expert level of knowledge;
- you give the DPO appropriate access to personal data and processing activities;
- you give the DPO appropriate access to other services within your organisation so that they can receive essential support, input or information;
- you seek the advice of your DPO when carrying out a DPIA; and

- you record the details of your DPO as part of your records of processing activities.

This shows the importance of the DPO to your organisation and that you must provide sufficient support so they can carry out their role independently. Part of this is the requirement for your DPO to report to the highest level of management. This doesn't mean the DPO has to be line managed at this level but they must have direct access to give advice to senior managers who are making decisions about personal data processing.

What details do we have to publish about the DPO?

The UK GDPR requires you to:

- publish the contact details of your DPO; and
- provide them to the ICO.

This is to enable individuals, your employees and the ICO to contact the DPO as needed. You aren't required to include the name of the DPO when publishing their contact details but you can choose to provide this if you think it's necessary or helpful.

You're also required to provide your DPO's contact details in the following circumstances:

- when consulting the ICO under Article 36 about a DPIA; and
- when providing [privacy information](#) to individuals under Articles 13 and 14.

However, remember you do have to provide your DPO's name if you report a [personal data breach](#) to the ICO and to those individuals affected by it.

Is the DPO responsible for compliance?

The DPO isn't personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the UK GDPR. Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 35-36, 37-39, 83 and Recital 97](#) 
External link

In more detail - ICO guidance

- See the following section of the [Guide to UK GDPR: Accountability and governance](#)
- See our [Guide to freedom of information](#)
- The [Accountability Framework](#) looks at the ICO's expectations in relation to leadership and oversight.

Data protection impact assessments

The Brexit transition period ended on 31 December 2020. The GDPR has been retained in UK law as the UK GDPR, and will continue to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law. If you transfer or receive data from overseas please visit our [End of Transition](#) and [International Transfers](#) pages. You should make sure you can identify any data you collected before the end of 2020 about people outside the UK, for further information, see our Q&A on Legacy Data.

On 01 January, there will not be any significant change to the UK data protection regime, or to the criteria that compel DPIAs. This guidance draws on European resources which we still consider to be relevant, and so these resources remain part of our DPIA guidance.

We will keep this guidance under review and update it as and when any aspect of your obligations or our approach changes. Please continue to monitor our website for updates.

- Click here for a sample [DPIA Template ↗](#)
- Click here to [contact the ICO about your DPIA](#)

At a glance

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:
 - describe the nature, scope, context and purposes of the processing;
 - assess necessity, proportionality and compliance measures;
 - identify and assess risks to individuals; and
 - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

- If you are processing for law-enforcement purposes, you should read this alongside the [Guide to Law Enforcement Processing](#).
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

Checklists

DPIA awareness checklist

- We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- Our existing policies, processes and procedures include references to DPIA requirements.
- We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- We have created and documented a DPIA process.
- We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

- We consider carrying out a DPIA in any major project involving the use of personal data.
- We consider whether to do a DPIA if we plan to carry out any other:
 - evaluation or scoring;
 - automated decision-making with significant effects;
 - systematic monitoring;
 - processing of sensitive data or data of a highly personal nature;
 - processing on a large scale;
 - processing of data concerning vulnerable data subjects;
 - innovative technological or organisational solutions;
 - processing that involves preventing data subjects from exercising a right or using a service or contract.
- We always carry out a DPIA if we plan to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
 - process special-category data or criminal-offence data on a large scale;
 - systematically monitor a publicly accessible place on a large scale;
 - use innovative technology in combination with any of the criteria in the European guidelines;
 - use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
 - carry out profiling on a large scale;
 - process biometric or genetic data in combination with any of the criteria in the European guidelines;
 - combine, compare or match data from multiple sources;
 - process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
 - process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
 - process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
 - process personal data that could result in a risk of physical harm in the event of a security breach.
- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist

- We describe the nature, scope, context and purposes of the processing.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our data protection officer.
- We check that the processing is necessary for and proportionate to our purposes, and describe

how we will ensure compliance with data protection principles.

- We do an [objective assessment](#) of the likelihood and severity of any risks to individuals' rights and interests.
- We identify measures we can put in place to eliminate or reduce high risks.
- We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We implement the measures we identified, and integrate them into our project plan.
- We consult the ICO before processing, if we cannot mitigate high risks.
- We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

We have:

- confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;
- explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;
- structured the document clearly, systematically and logically;
- written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;
- set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;
- ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;
- explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);
- explained how we plan to support the relevant information rights of our data subjects;

- identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;
- explained sufficiently how any proposed mitigation reduces the identified risk in question;
- evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;
- given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;
- attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;
- recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;
- agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;
- consulted the ICO if there are residual high risks we cannot mitigate.

In brief

- [What is a DPIA?](#)
- [When do we need a DPIA?](#)
- [How do we carry out a DPIA?](#)
- [Do we need to consult the ICO?](#)
- [In more detail](#)

What is a DPIA?

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and

building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise. You should see it as an ongoing process that is subject to regular review.

When do we need a DPIA?

You must do a DPIA before you begin any type of processing that is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

When considering if your processing is likely to result in high risk, you should consider the relevant [European guidelines](#). These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

The ICO also requires you to do a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new

project involving the use of personal data. You can use or adapt the [checklists](#) to help you carry out this screening exercise.

How do we carry out a DPIA?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process.

The process is designed to be flexible and scalable. You can use or adapt our [sample DPIA template ↗](#), or create your own. If you want to create your own, you may want to refer to the European guidelines which set out [Criteria for an acceptable DPIA ↗](#).

Although publishing a DPIA is not a requirement of UK GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, where possible, removing sensitive details if necessary.

Do we need to consult the ICO?

You don't need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a high risk and you cannot take measures to reduce that

risk. You cannot begin the processing until you have consulted us.

If you want your project to proceed effectively then investing time in producing a comprehensive DPIA may prevent any delays later, if you have to consult with the ICO.

You need to [send us](#) a copy of your DPIA.

Once we have the information we need, we will generally respond within eight weeks (although we can extend this by a further six weeks in complex cases).

We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal warning or take action to ban the processing altogether.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95](#) 
External link

 [Joint Surveillance Camera Commissioner /ICO guidance on Data protection impact assessments for surveillance camera systems](#) 
External link

In more detail – ICO guidance

We have published [more detailed guidance on DPIAs](#).

The [Accountability Framework](#) looks at the ICO's expectations in relation to DPIAs.

In more detail – European Data Protection Board

- WP29 produced [guidelines on data protection impact assessments](#), which have been endorsed by the EDPB.
- Other relevant guidelines include:
- [Guidelines on Data Protection Officers \('DPOs'\)](#) (WP243)
- [Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679](#) (WP251)

Data protection by design and default

At a glance

- The UK GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the UK GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Checklists

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and

organisational measures for data protection by design.

- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

In brief

- [What does the UK GDPR say about data protection by design and by default?](#)
- [What is data protection by design?](#)
- [What is data protection by default?](#)
- [Who is responsible for complying with data protection by design and by default?](#)
- [What are we required to do?](#)
- [When should we do this?](#)
- [What are the underlying concepts of data protection by design and by default?](#)
- [How do we do this in practice?](#)
- [How does data protection by design and by default link to data protection impact assessments \(DPIAs\)?](#)
- [What is the role of privacy-enhancing technologies \(PETs\)?](#)
- [What about international transfers?](#)
- [What is the role of certification?](#)
- [What additional guidance is available?](#)

What does the UK GDPR say about data protection by design and by default?

The UK GDPR requires you to integrate data protection concerns into every aspect of your processing activities. This approach is 'data protection by design and by default'. It is a key element of the UK GDPR's risk-based approach and its focus on accountability, ie your ability to demonstrate how you are complying with its requirements.

Some organisations already adopt a 'privacy by design approach' as a matter of good practice. If this is the case for you, then you are well-placed to meet the requirements of data protection by design and by default. However, you may still need to review your processes and procedures to ensure that you are meeting your obligations.

Articles 25(1) and 25(2) of the GDPR outline your obligations concerning data protection by design and by default.

Article 25(1) specifies the requirements for data protection by design:

“

‘Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.’

Article 25(2) specifies the requirements for data protection by default:

“

‘The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.’

Article 25(3) states that if you adhere to an approved certification under Article 42, you can use this as one way of demonstrating your compliance with these requirements.

Further Reading

 [Relevant provisions in the UK GDPR - Article 25 and Recital 78](#) 

External link

What is data protection by design?

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the UK GDPR, it requires you to:

- put in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and
- integrate safeguards into your processing so that you meet the UK GDPR's requirements and protect individual rights.

In essence this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices.

Data protection by design has broad application. Examples include:

- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- physical design;
- embarking on data sharing initiatives; or
- using personal data for new purposes.

The underlying concepts of data protection by design are not new. Under the name 'privacy by design' they have existed for many years.

What is data protection by default?

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of [data minimisation](#) and [purpose limitation](#).

You have to process some personal data to achieve your purpose(s). Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose. It does **not** require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

Nevertheless, you must consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.

Who is responsible for complying with data protection by design and by default?

Article 25 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. Depending on your circumstances, you may have different requirements for different areas within your organisation. For example:

- your senior management, eg developing a culture of 'privacy awareness' and ensuring you develop policies and procedures with data protection in mind;
- your software engineers, system architects and application developers, eg those who design systems, products and services should take account of data protection requirements and assist you in complying with your obligations; and
- your business practices, eg you should ensure that you embed data protection by design in all your internal processes and procedures.

This may not apply to all organisations, of course. However, data protection by design is about adopting an

organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity you undertake. It doesn't apply only if you are the type of organisation that has your own software developers and systems architects.

In considering whether to impose a penalty, the ICO will take into account the technical and organisational measures you have put in place in respect of data protection by design. Additionally, under the Data Protection Act 2018 (DPA 2018) we can issue an Enforcement Notice against you for any failings in respect of Article 25.

What about data processors?

If you use another organisation to process personal data on your behalf, then that organisation is a data processor under the UK GDPR.

Article 25 does not mention data processors specifically. However, Article 28 specifies the considerations you must take whenever you are selecting a processor. For example, you must only use processors that provide:

“

'sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'

This requirement covers both data protection by design in Article 25 as well as other aspects (eg your security obligations under Article 32). Your processor cannot necessarily assist you with your data protection by design obligations (unlike with security measures), however you must only use processors that provide sufficient guarantees to meet the UK GDPR's requirements.

What about other parties?

Data protection by design and by default can also impact organisations other than controllers and processors. Depending on your processing activity, other parties may be involved, even if this is just where you purchase a product or service that you then use in your processing. Examples include manufacturers, product developers, application developers and service providers.

Recital 78 extends the concepts of data protection by design to other organisations, although it does not place a requirement on them to comply – that remains with you as the controller. It says:

“

'When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.'

Therefore, when considering what products and services you need for your processing, you should look to choose those where the designers and developers have taken data protection into account. This can help to ensure that your processing adheres to the data protection by design requirements.

If you are a developer or designer of products, services and applications, the UK GDPR places no specific obligations on you about how you design and build these products. (You may have specific obligations as a controller in your own right, eg for any employee data.) However, you should note that controllers are required to consider data protection by design when selecting services and products for use in their data processing activities – therefore if you design these products with data protection in mind, you may be in a better position.

Further Reading

 [Relevant provisions in the UK GDPR - Articles 25 and 28, and Recitals 78, 79, 81 and 82](#) 

External link

What are we required to do?

You must put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and safeguard individual rights.

There is no 'one size fits all' method to do this, and no one set of measures that you should put in place. It depends on your circumstances.

The key is that you consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Some examples of how you can do this include:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

This is not an exhaustive list. Complying with data protection by design and by default may require you to do much more than the above.

However, we cannot provide a complete guide to all aspects of data protection by design and by default in all circumstances. This guidance identifies the main points for you to consider. Depending on the processing you are doing, you may need to obtain specialist advice that goes beyond the scope of this guidance.

Further Reading

 [Relevant provisions in the UK GDPR - Recital 78](#) 

External link

When should we do this?

Data protection by design starts at the initial phase of any system, service, product, or process. You should begin by considering your intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure that you comply with the data protection principles and protect individual rights. These considerations must cover:

- the state of the art and costs of implementation of any measures;
- the nature, scope, context and purposes of your processing; and
- the risks that your processing poses to the rights and freedoms of individuals.

This is similar to the information risk assessment you should do when considering your security measures.

These considerations lead into the second step, where you put in place actual technical and organisational measures to implement the data protection principles and integrate safeguards into your processing.

This is why there is no single solution or process that applies to every organisation or every processing activity, although there are a number of commonalities that may apply to your specific circumstances as described below.

The UK GDPR requires you to take these actions:

- 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- 'at the time of the processing itself' – ie during the lifecycle of your processing activity.

What are the underlying concepts of data protection by design and by default?

The underlying concepts are essentially expressed in the seven 'foundational principles' of privacy by design, as developed by the Information and Privacy Commissioner of Ontario.

Although privacy by design is not necessarily equivalent to data protection by design, these foundational principles can nevertheless underpin any approach you take.

'Proactive not reactive; preventative not remedial'

You should take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact. This doesn't just apply in the context of systems design – it involves developing a culture of 'privacy awareness' across your organisation.

'Privacy as the default setting'

You should design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.

'Privacy embedded into design'

Embed data protection into the design of any systems, services, products and business practices. You should ensure data protection forms part of the core functions of any system or service – essentially, it

becomes integral to these systems and services.

'Full functionality – positive sum, not zero sum'

Also referred to as 'win-win', this principle is essentially about avoiding trade-offs, such as the belief that in any system or service it is only possible to have privacy **or** security, not privacy **and** security. Instead, you should look to incorporate all legitimate objectives whilst ensuring you comply with your obligations.

'End-to-end security – full lifecycle protection'

Put in place strong security measures from the beginning, and extend this security throughout the 'data lifecycle' – ie process the data securely and then destroy it securely when you no longer need it.

'Visibility and transparency – keep it open'

Ensure that whatever business practice or technology you use operates according to its premises and objectives, and is independently verifiable. It is also about ensuring visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.

'Respect for user privacy – keep it user-centric'

Keep the interest of individuals paramount in the design and implementation of any system or service, eg by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

How do we do this in practice?

One means of putting these concepts into practice is to develop a set of practical, actionable guidelines that you can use in your organisation, framed by your assessment of the risks posed and the measures available to you. You could base these upon the seven foundational principles.

However, how you go about doing this depends on your circumstances – who you are, what you are doing, the resources you have available, and the nature of the data you process. You may not need to have a set of documents and organisational controls in place, although in some situations you will be required to have certain documents available concerning your processing.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- you consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- you make data protection an essential component of the core functionality of your processing systems and services;
- you only process the personal data that you need in relation to your purposes(s), and that you only use the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- the identity and contact information of those responsible for data protection are available both within

your organisation and to individuals;

- you adopt a ‘plain language’ policy for any public documents so that individuals easily understand what you are doing with their personal data;
- you provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and
- you offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

Many of these relate to other obligations in the UK GDPR, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of data protection by design and how it applies to all aspects of your processing. Our guidance on these topics will help you when you consider the measures you need to put in place for data protection by design and by default.

In more detail – ICO guidance

Read our sections on [the data protection principles](#), [individual rights](#), [accountability and governance](#), [documentation](#), [data protection impact assessments](#), [data protection officers](#) and [security](#).

The [Accountability Framework](#) looks at the ICO’s expectations in relation to data protection by design.

In more detail – European Data Protection Board

The European Data Protection Board (EDPB) adopts guidelines for complying with the requirements of the EU GDPR.

The EDPB has adopted guidelines on [Data Protection by Design and Default](#).

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Further reading

We will produce further guidance on how you can implement data protection by design soon. However, the Information and Privacy Commissioner of Ontario has published [guidance on how organisations can ‘operationalise’ privacy by design](#), which may assist you.

How does data protection by design and by default link to data protection impact assessments (DPIAs)?

A DPA is a tool that you can use to identify and reduce the data protection risks of your processing activities. They can also help you to design more efficient and effective processes for handling personal data.

DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organisational measures you need in order to ensure your processing complies with the data protection principles.

However, a DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to rights and freedoms, though it is good practice to undertake a DPIA anyway. In contrast, data protection by design is a broader concept, as it applies organisationally and requires you to take certain considerations even before you decide whether your processing is likely to result in a high risk or not.

What is the role of privacy-enhancing technologies (PETs)?

Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals. A useful definition from the European Union Agency for Cybersecurity (ENISA) refers to PETs as:

“

‘software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.’

PETs link closely to the concept of privacy by design, and therefore apply to the technical measures you can put in place. They can assist you in complying with the data protection principles and are a means of implementing data protection by design within your organisation on a technical level.

Further reading

We will provide further guidance on PETs in the near future. ENISA has also published [research reports](#) on PETs that may assist you.

What about international transfers?

Data protection by design also applies in the context of international transfers in cases where you intend to transfer personal data overseas to a third country that does not have an adequacy decision.

You need to ensure that, whatever mechanism you use, appropriate safeguards are in place for these transfers. As detailed in Recital 108, these safeguards need to include compliance with data protection by design and by default.

Further Reading

 [Relevant provisions in the UK GDPR - Article 47 and Recital 108](#) 

External link

In more detail – ICO guidance

Read our guidance on [international transfers](#).

What is the role of certification?

Article 25(3) says that:

“

‘An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.’

This means that being certified through an [ICO approved certification scheme](#) can assist you in showing how you are complying with, and implementing, data protection by design and by default.

What additional guidance is available?

The ICO will publish more detailed guidance about data protection by design and privacy enhancing technologies soon, as well as how these concepts apply in the context of the [code of practice](#) on age appropriate design in the DPA 2018 section 123.

In the meantime, there are a number of publications about the privacy by design approach. We have summarised some of these below.

Documentation

At a glance

- The UK GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the UK GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

Checklists

Documentation of processing activities – requirements

If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the UK GDPR.

If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the UK GDPR.

If we process special category or criminal conviction and offence data, we document:

the condition for processing we rely on in the Data Protection Act 2018 (DPA 2018);

the lawful basis for our processing; and

whether we retain and erase the personal data in accordance with our policy document.

where required in schedule 1 of the DPA 2018.

We document our processing activities in writing.

We document our processing activities in a granular way with meaningful links between the different pieces of information.

- We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

- do information audits to find out what personal data our organisation holds;
- distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and
- review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
 - records of consent;
 - controller-processor contracts;
 - the location of personal data;
 - Data Protection Impact Assessment reports; and
 - records of personal data breaches.
- We document our processing activities in electronic form so we can add, remove and amend information easily.

In brief

- [What is documentation?](#)
- [Who needs to document their processing activities?](#)
- [What do we need to document under Article 30 of the GDPR?](#)
- [Should we document anything else?](#)
- [How do we document our processing activities?](#)
- [In detail](#)

What is documentation?

- Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.
- Documenting your processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other

aspects of the UK GDPR.

Who needs to document their processing activities?

- Controllers and processors each have their own documentation obligations.
- If you have 250 or more employees, you must document all your processing activities.
- There is a limited exemption for small and medium-sized organisations. If you have fewer than 250 employees, you only need to document processing activities that:
 - are not occasional; or
 - could result in a risk to the rights and freedoms of individuals; or
 - involve the processing of special categories of data or criminal conviction and offence data.

What do we need to document under Article 30 of the UK GDPR?

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the UK GDPR and the UK's Data Protection Act 2018. Such documentation may include:

- information required for privacy notices, such as:
 - the lawful basis for the processing
 - the legitimate interests for the processing
 - individuals' rights
 - the existence of automated decision-making, including profiling
 - the source of the personal data;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;

- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018, covering:
 - the condition for processing in the Data Protection Act;
 - the lawful basis for the processing in the UK GDPR; and
 - your retention and erasure policy document.

How do we document our processing activities?

- Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.
- You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.
- When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

We have developed basic templates to help you document your processing activities.

Further Reading

Documentation template for controllers

For organisations
File (31.22K)

Documentation template for processors

For organisations
File (19.48K)

Further Reading

Relevant provisions in the UK GDPR – See Article 30 and Recital 82

External link

Relevant provisions in the Data Protection Act 2018 – See Schedule 1

External link

In more detail – ICO guidance

We have produced [more detailed guidance on documentation](#).

The [Accountability Framework](#) looks at the ICO's expectations in relation to records of processing.

Contracts

At a glance

- Whenever a controller uses a processor, there must be a written contract (or other legal act) in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The UK GDPR sets out what needs to be included in the contract.
- If a processor uses another organisation (ie a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

Checklists

What to include in the contract

The contract (or other legal act) sets out details of the processing including:

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject;
- the controller's obligations and rights.

The contract or other legal act includes terms or clauses stating that:

- the processor must only act on the controller's documented instructions, unless required by law to act without such instructions;
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract;
- the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;

- taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and
- the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.

In brief

- When is a contract needed and why is it important?
- What needs to be included in the contract?
- What responsibilities and liabilities do controllers have when using a processor?
- What responsibilities and liabilities do processors have in their own right?
- In more detail

When is a contract needed and why is it important?

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties.

Similarly, if a processor uses another organisation (ie a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the UK GDPR, and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

What needs to be included in the contract?

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;

- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the UK GDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the UK GDPR. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to Article 28(3) must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 28, 29, 30, 31, 32, 33, 34, 35 and 36 and Recitals 81, 82 and 83](#) 
External link

In more detail – ICO guidance

We have produced more detailed guidance on [contracts and liabilities between controllers and processors](#) .

The [Accountability Framework](#) looks at the ICO's expectations in relation to contracts.

Security

At a glance

- A key principle of the UK GDPR is that you process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle’.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the ‘confidentiality, integrity and availability’ of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
- We have worked closely with the National Cyber Security Centre (NCSC) to develop [an approach](#) that you can use when assessing the measures that will be appropriate for you.

Checklists

- We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have assessed what we need to do by considering the [security outcomes](#) we want to achieve.
- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

In brief

- [What does the UK GDPR say about security?](#)
- [Why should we worry about information security?](#)
- [What do we need to protect with our security measures?](#)
- [What level of security is required?](#)
- [What organisational measures do we need to consider?](#)
- [What technical measures do we need to consider?](#)
- [What if we operate in a sector that has its own security requirements?](#)
- [What do we do when a data processor is involved?](#)
- [Should we use pseudonymisation and encryption?](#)
- [What are ‘confidentiality, integrity, availability’ and ‘resilience’?](#)
- [What are the requirements for restoring availability and access to personal data?](#)
- [Are we required to ensure our security measures are effective?](#)
- [What about codes of conduct and certification?](#)
- [What about our staff?](#)

What does the UK GDPR say about security?

Article 5(1)(f) of the UK GDPR concerns the ‘integrity and confidentiality’ of personal data. It says that personal data shall be:

“

'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

You can refer to this as the UK GDPR's 'security principle'. It concerns the broad concept of **information security**.

This means that you must have appropriate security in place to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

You need to consider the security principle alongside Article 32 of the UK GDPR, which provides more specifics on the security of your processing. Article 32(1) states:

“

'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5(1)(f) and 32, and Recitals 39 and 83 
External link

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;

- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.

The ICO is also required to consider the technical and organisational measures you had in place when considering an administrative fine.

What do our security measures need to protect?

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the UK GDPR, they form part of your obligations.

What level of security is required?

The UK GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects both the UK GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

Further Reading

↗ Relevant provisions in the UK GDPR - See Article 32(2) and Recital 83 ↘

External link

We cannot provide a complete guide to all aspects of security in all circumstances for all organisations, but this guidance is intended to identify the main points for you to consider.

What organisational measures do we need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you will need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively.

Example

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Clear accountability for security will ensure that you do not overlook these issues, and that your overall security posture does not become flawed or out of date.

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (eg the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside your organisation (eg for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- periodic checks to ensure that your security measures remain appropriate and up to date.

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it's also the case that you may not need a great deal of time and resources to secure your systems and the personal data they process.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;
- you should take into account the state of technological development, but you are also able to consider the costs of implementation;
- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

A good starting point is to make sure that you're in line with the requirements of Cyber Essentials – a government scheme that includes a set of basic technical controls you can put in place relatively easily.

You should however be aware that you may have to go beyond these requirements, depending on your processing activities. Cyber Essentials is only intended to provide a 'base' set of controls, and won't address the circumstances of every organisation or the risks posed by every processing operation.

A list of helpful sources of information about cybersecurity is provided below.

Further reading – ICO/NCSC security outcomes

We have worked closely with the NCSC to develop a set of [security outcomes](#) that you can use to determine the measures appropriate for your circumstances.

The [Accountability Framework](#) looks at the ICO's expectations in relation to security.

Further reading – ICO guidance

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. Where appropriate, we will be updating each of these to reflect the UK GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider.

- [IT asset disposal for organisations](#) (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- [A practical guide to IT security – ideal for the small business](#) (pdf);
- [Protecting personal data in online services – learning from the mistakes of others](#) (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework;
- [Bring your own device \(BYOD\)](#) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data;
- [Cloud computing](#) (pdf) – guidance covering how security requirements apply to personal data processed in the cloud; and
- [Detailed guidance on encryption](#) – advice on the use of encryption to protect personal data.

Other resources

[Homepage of the Cyber Essentials scheme](#)

What if we operate in a sector that has its own security requirements?

Some industries have specific security requirements or require you to adhere to certain frameworks or standards. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators. If you operate in these sectors, you need to be aware of their requirements, particularly if specific technical measures are specified.

Although following these requirements will not necessarily equate to compliance with the UK GDPR's security principle, the ICO will nevertheless consider these carefully in any considerations of regulatory action. It can be the case that they specify certain measures that you should have, and that those measures contribute to your overall security posture.

Example

If you are processing payment card data, you are obliged to comply with the [Payment Card Industry Data Security Standard ↗](#). The PCI-DSS outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the UK GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

What do we do when a processor is involved?

If one or more organisations process personal data on your behalf, then these are data processors under the UK GDPR. This can have the potential to cause security problems – as a data controller you are responsible for ensuring compliance with the UK GDPR and this includes what the processor does with the data. However, in addition to this, the UK GDPR's security requirements also apply to any processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its security measures;
- your written contract must stipulate that the processor takes all measures required under Article 32 – basically, the contract has to require the processor to undertake the same security measures that you would have to take if you were doing the processing yourself; and
- you should ensure that your contract includes a requirement that the processor makes available all information necessary to demonstrate compliance. This may include allowing for you to audit and inspect the processor, either yourself or an authorised third party.

At the same time, your processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 28 and 32, and Recitals 81 and 83 ↗](#)

External link

Further reading

[Controllers and processors](#)

[Contracts](#)

Should we use pseudonymisation and encryption?

Pseudonymisation and encryption are specified in the UK GDPR as two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. It depends on the nature, scope, context and purposes of your processing, and the risks posed to individuals.

However, there are a wide range of solutions that allow you to implement both without great cost or difficulty. For example, for a number of years the ICO has considered encryption to be an appropriate technical measure given its widespread availability and relatively low cost of implementation. This position has not altered due to the UK GDPR — if you are storing personal data, or transmitting it over the internet, we recommend that you use encryption and have a suitable policy in place, taking account of the residual risks involved.

When considering what to put in place, you should undertake a risk analysis and document your findings.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 32\(1\)\(a\) and Recital 83](#) 

External link

In more detail – ICO guidance

[Detailed guidance on encryption](#)

What are ‘confidentiality, integrity, availability’ and ‘resilience’?

Collectively known as the ‘CIA triad’, confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

The CIA triad has existed for a number of years and its concepts are well-known to security professionals.

You are also required to have the ability to ensure the ‘resilience’ of your processing systems and services. Resilience refers to:

- whether your systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
- your ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

Further Reading

 Relevant provisions in the UK GDPR - See Article 32(1)(b) and Recital 83 

External link

What are the requirements for restoring availability and access to personal data?

You must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a 'timely manner'.

The UK GDPR does not define what a 'timely manner' should be. This therefore depends on:

- who you are;
- what systems you have; and
- the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.

The key point is that you have taken this into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.

Example

An organisation takes regular backups of its systems and the personal data held within them. It follows the well-known '3-2-1' backup strategy: three copies, with two stored on different devices and one stored off-site.

The organisation is targeted by a ransomware attack that results in the data being encrypted. This means that it is no longer able to access the personal data it holds.

Depending on the nature of the organisation and the data it processes, this lack of availability can have significant consequences on individuals – and would therefore be a personal data breach under the UK GDPR.

The ransomware has spread throughout the organisation's systems, meaning that two of the backups are also unavailable. However, the third backup, being stored off-site, allows the organisation to restore its systems in a timely manner. There may still be a loss of personal data depending on when the off-site backup was taken, but having the ability to restore the systems means that whilst there will be

some disruption to the service, the organisation are nevertheless able to comply with this requirement of the UK GDPR.

Further Reading

 Relevant provisions in the UK GDPR - See Article 32(1)(c) and Recital 83 

External link

Are we required to ensure our security measures are effective?

Yes, the UK GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place. What these tests look like, and how regularly you do them, will depend on your own circumstances. However, it's important to note that the requirement in the UK GDPR concerns your measures in their entirety, therefore whatever 'scope' you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essentially 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve.

In some industries, you are required to undertake tests of security measures on a regular basis. The UK GDPR now makes this an obligation for all organisations. Importantly, it does not specify the type of testing, nor how regularly you should undertake it. It depends on your organisation and the personal data you are processing.

You can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

Further Reading

 Relevant provisions in the UK GDPR - See Article 32(1)(d) and Recital 83 

External link

What about codes of conduct and certification?

If your security measures include a product or service that adheres to a UK GDPR code of conduct or certification scheme, you may be able to use this as an element to demonstrate your compliance with the security principle. It is important that you check carefully that the code or certification scheme has been approved by the ICO.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(3) and Recital 83

External link

Further reading

[Codes of conduct](#)

[Certification](#)

What about our staff?

The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, including:

- your responsibilities as a data controller under the UK GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (eg to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(4) and Recital 83

External link

Other resources

The NCSC has detailed [technical guidance](#) in a number of areas that will be relevant to you whenever you process personal data. Some examples include:

- [10 Steps to Cyber Security](#) – The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.

Security outcomes

At a glance

- The UK GDPR requires you to process personal data securely using appropriate technical and organisational measures.
- What's appropriate for you will depend not just on your circumstances, but also the data you are processing and the risks posed.
- You must assess your information security risk and implement appropriate technical controls.
- The Information Commissioner's Office and the National Cyber Security Centre (NCSC) have worked together to develop an approach that you can use when making this assessment.
- It allows you to consider common expectations and either follow existing guidance, use particular services or develop your own processes if you have appropriate knowledge and resources to do so.
- The approach is based on four aims:
 - managing security risk;
 - protecting personal data against cyber-attack;
 - detecting security events; and
 - minimising the impact.

In brief

- [What does the UK GDPR say about security?](#)
- [What are the other requirements?](#)
- [How does security relate to the GDPR's accountability principle and our responsibility as data controllers?](#)
- [What are 'appropriate technical and organisational measures'?](#)
- [Why 'security outcomes'?](#)
- [What are the aims?](#)
- [What are the outcomes?](#)
 - [A. Manage your security risk](#)
 - [B. Protect personal data against cyber-attack](#)
 - [C. Detect security events](#)
 - [D. Minimise the impact](#)

What does the UK GDPR say about security?

The UK GDPR requires you to process personal data securely. Article 5(1)(f) concerns 'integrity and confidentiality' of personal data - in short, it is the GDPR's 'security principle'. It states that personal data shall be:

“

'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

The aim of this guidance is to describe an overall set of outcomes that are considered 'appropriate' to prevent personal data being accidentally or deliberately compromised.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5(1)(f) and Recital 39 

External link

In more detail — ICO guidance

- Security

What are the other requirements?

Alongside the security principle, the UK GDPR contains other relevant requirements, including data protection by design in Article 25 and security of processing in Article 32.

Data protection by design requires you to put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and integrate necessary safeguards into the processing. You have to do this at the time of the determination of the means of the processing (ie the design phase of any processing operation) and at the time of the processing itself.

You also have specific security obligations under Article 32 which apply whether you are a controller or a processor. These require you to put in place appropriate technical and organisational measures to ensure an appropriate level of security of both the processing and your processing environment.

These provisions cover fundamental information security concepts including:

- minimisation of personal data collected;
- managing, limiting and controlling access to personal data;
- protecting the classic 'CIA triad' (confidentiality, integrity, and availability) of personal data;
- resilience of processing systems and services, and the ability to restore availability and access to personal data; and
- regular testing of the effectiveness of measures implemented.

The measures you implement should be appropriate to the risk presented.

Further Reading

 Relevant provisions in the UK GDPR See Articles 25 and 32, and Recitals 78 and 83 

External link

In more detail – ICO guidance

- Data protection by design
- Security

How does security relate to the UK GDPR's accountability principle and our responsibility as data controllers?

The accountability principle requires you to be able to demonstrate that your processing is done in compliance with the UK GDPR. Accountability also has direct relevance to your responsibility as a data controller.

You are required to implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing of personal data is performed in accordance with the UK GDPR.

Further Reading

 Relevant provisions in the UK GDPR See Article 5(2) and 24, and Recital 74 

External link

In more detail – ICO guidance

- Accountability and governance

What are ‘appropriate technical and organisational measures’?

The UK GDPR requires you to have a level of security that is ‘appropriate’ to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing. This reflects both the UK GDPR’s risk-based approach, and that there is no ‘one size fits all’ solution to information security.

This means that what’s ‘appropriate’ for you will depend on your own circumstances, the processing you’re doing, and the risks it presents to your organisation.

This guidance sets out a set of security outcomes that could form the basis of describing ‘appropriate technical and organisational measures’ to protect personal data. Whilst there are minimum expectations, the precise implementation of any measures must be appropriate to the risks you face.

In more detail – ICO guidance

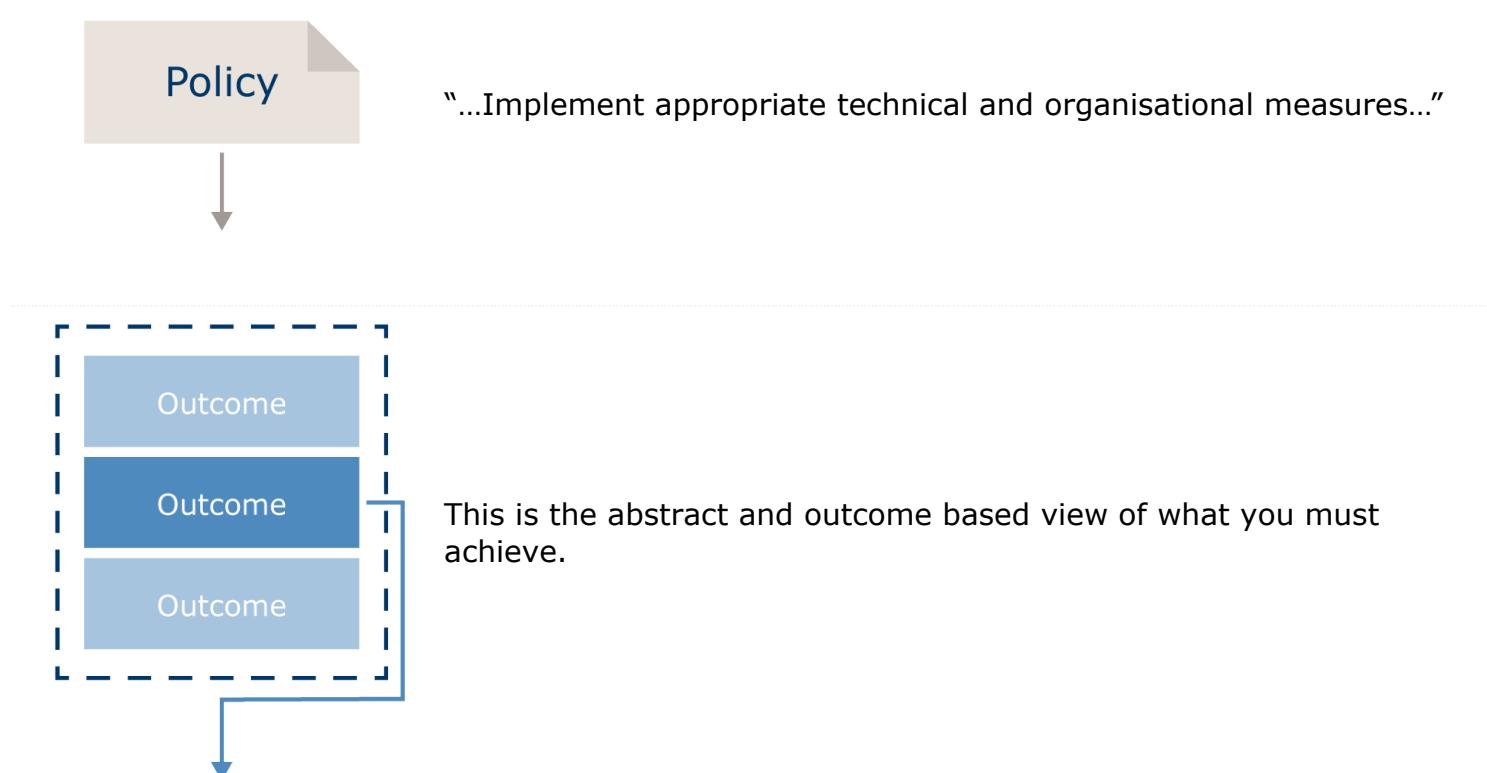
- Security

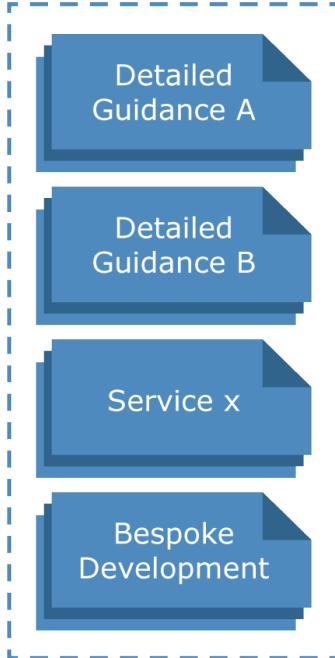
Why ‘security outcomes’?

It may seem like there is a lot of confusion as to the technical security required to comply with your data protection obligations. There is lots of detailed guidance available, but it may not be immediately clear what you must put in place, what is simply a suggested approach and what is relevant to you and your circumstances.

The outcomes intend to provide a common set of expectations that you can meet, either through following existing guidance, using particular services or, if you are sufficiently competent, development of your own bespoke approach.

An outcomes-based approach also enables scaling to any size or complexity of organisation or data processing operation. The outcomes remain constant – it is how they are implemented that differs.





Detailed guidance showing examples of how to achieve the outcomes or perhaps appropriate services may be available to procure, or alternatively a competent organisation might develop a bespoke approach.

What are the aims?

The approach has been developed in accordance with the following four aims:

- A) manage your security risk;
- B) protect personal data against cyber-attack,
- C) detect security events; and
- D) minimise the impact.

Each outcome is summarised under its respective aim, with specific reference to the data protection context following.

What are the outcomes?

A. Manage your security risk

You have appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to personal data.

A.1 Governance

You have appropriate data protection and information security policies and processes in place. If required, you ensure that you maintain records of processing activities and have appointed a Data Protection Officer.

In more detail — ICO guidance

The ICO has published guidance on [data protection officers](#), [accountability and governance](#), [documentation](#) and [security](#).

In more detail—Article 29

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of EU version of the GDPR.

WP29 published [guidelines on Data Protection Officers](#), which the EDPB endorsed in May 2018.

A.2 Risk management

You take appropriate steps to identify, assess and understand security risks to personal data and the systems that process this data.

The UK GDPR emphasises a risk-based approach to data protection and the security of your processing systems and services. You must take steps to assess these risks and include appropriate organisational measures to make effective risk-based decisions based upon:

- the state of the art (of technology);
- the cost of implementation;
- the nature, scope, context and purpose of processing; and
- the severity and likelihood of the risk(s).

Beyond this, where the processing is likely to result in a high risk to the rights and freedoms of individuals, you must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, you need to have a process in place to consult with the ICO before you start the processing.

In more detail — ICO guidance

- [DPIAs](#)

In more detail—Article 29

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29),

includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of EU version of the GDPR.

WP29 produced [guidelines on high risk processing and DPIAs](#), which the EDPB endorsed in May 2018.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Other resources

The NCSC has guidance on [risk management for cyber security](#). Additionally, [Step 1](#) of the 10 Steps to Cyber Security is about developing an information risk management regime.

A.3 Asset management

You understand and catalogue the personal data you process and can describe the purpose for processing it. You also understand the risks posed to individuals of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data.

The personal data you process should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary.

A.4 Processors and the supply chain

You understand and manage security risks to your processing operations that may arise as a result of using third parties such as data processors. This includes ensuring that they employ appropriate security measures.

In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The UK GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.

In more detail — ICO guidance

- [Controllers and processors](#)
- [Contracts](#)

Other resources

The NCSC has also published [guidance on managing cyber risks](#) in your supply chain.

B. Protect personal data against cyber-attack

You have proportionate security measures in place to protect against cyber-attack which cover:

- the personal data you process; and
- the systems that process such data.

B.1 Service protection policies and processes

You should define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems involved in the processing of personal data.

You should also consider assessing your systems and implementing specific technical controls as laid out in appropriate frameworks (such as Cyber Essentials).

Other resources

Homepage of the [Cyber Essentials schemes](#) at the NCSC's website.

B.2 Identity and access control

You understand, document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

You should appropriately authenticate and authorise users (or any automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.

You should prevent users from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. You should appropriately constrain legitimate access and ensure there is an appropriate audit trail.

You should have a robust password policy which avoids users having weak passwords, such as those trivially guessable. You should change all default passwords and remove or suspend unused accounts.

B.3 Data security

You implement technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.

B.4 System security

You implement appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber-attack.

Whilst the UK GDPR requires a risk-based approach, typical examples of security measures you could take

include:

- tracking and recording all assets that process personal data, including end user devices and removable media;
- minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity;
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), and taking other mitigating steps, where patches can't be applied;
- managing end user devices (laptops and smartphones etc.) so that you can apply organisational controls over software or applications that interact with or access personal data;
- encrypting personal data at rest on devices (laptops, smartphones, removable media) that are not subject to strong physical controls;
- encrypting personal data when transmitted electronically;
- ensuring that web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications such as the OWASP Top 10; and
- ensuring your processing environment remains secure throughout its lifecycle.

You also undertake regular testing to evaluate the effectiveness of your security measures, including virus and malware scanning, vulnerability scanning and penetration testing as appropriate. You record the results of any testing and remediating action plans.

Whatever security measures you put in place – whether these are your own, or whether you use a third party service such as a cloud provider – you remain responsible both for the processing itself, and also in respect of any devices that you operate.

Further reading — ICO guidance

- [Security](#)
- [Encryption](#)
- [Passwords in online services](#)

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. Where appropriate, we will be updating each of these to reflect the UK GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider:

- [IT security top tips](#) – for further general information on IT security;
- [IT asset disposal for organisations](#) (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- [A practical guide to IT security – ideal for the small business](#) (pdf);
- [Protecting personal data in online services – learning from the mistakes of others](#) (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework;
- [Bring your own device \(BYOD\)](#) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data; and
- [Cloud computing](#) (pdf) – guidance covering how security requirements apply to personal data

processed in the cloud.

Other resources

- The NCSC has detailed technical guidance [\(external link\)](#) in a number of areas that will be relevant to you whenever you process personal data. Some examples include:
- [10 Steps to Cyber Security](#) [\(external link\)](#) - The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.
- Guidance on cybersecurity for [small businesses](#) [\(external link\)](#) and for [charities](#) [\(external link\)](#);
- [Using passwords to protect your data](#) [\(external link\)](#);
- [Penetration testing](#) [\(external link\)](#);
- Guidance on end-user device security; and
- Guidance on keeping your smartphones and tablets safe [\(external link\)](#).

The OWASP Foundation maintains the [OWASP Top 10](#) [\(external link\)](#).

The European Union Agency for Cybersecurity (ENISA) also has [guidance on data protection and security](#) [\(external link\)](#), including a '[Handbook](#) [\(external link\)](#)' on security of personal data and [guidelines for SMEs](#) [\(external link\)](#).

B.5 Staff awareness and training

You give your staff appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data.

Staff should be provided support so that they do not inadvertently process personal data (eg by sending it to the incorrect recipient).

Other resources

[10 Steps to Cyber Security](#) is about user education and awareness [\(external link\)](#).

C. Detect security events

You can detect security events that affect the systems that process personal data and you monitor authorised user access to that data.

C.1 Security monitoring

You appropriately monitor the status of systems processing personal data and monitor user access to personal data, including anomalous user activity.

You record user access to personal data. Where unexpected events or indications of a personal data breach

are detected, you have processes in place to act upon those events as necessary in an appropriate timeframe.

Other resources

[10 Steps to Cyber Security](#) is about monitoring ↗.

D. Minimise the impact

You can:

- minimise the impact of a personal data breach;
- restore your systems and services;
- manage the incident appropriately; and
- learn lessons for the future.

D.1 Response and recovery planning

You have well-defined and tested incident management processes in place in case of personal data breaches. You have mitigation processes in place that are designed to contain or limit the range of personal data that could be compromised following a personal data breach.

Where the loss of availability of personal data could cause harm, you have measures in place to ensure appropriate recovery. This should include maintaining (and securing) appropriate backups.

Other resources

NCSC guidance on [backing up your data](#) ↗.

D.2 Improvements

When a personal data breach occurs, you take steps to:

- understand the root cause;
- report the breach to the ICO and, where appropriate, affected individuals;
- where appropriate (or required), report to other relevant bodies (for example, other regulators, the NCSC and/or law enforcement); and
- take appropriate remediating action.

Further reading – ICO guidance

- [Personal data breaches](#)

Passwords in online services

At a glance

- Although the UK GDPR does not say anything specific about passwords, you are required to process personal data securely by means of appropriate technical and organisational measures.
- Passwords are a commonly-used means of protecting access to systems that process personal data. Therefore, any password setup that you implement must be appropriate to the particular circumstances of this processing.
- You should consider whether there are any better alternatives to using passwords.
- Any password system you deploy must protect against theft of stored passwords and 'brute-force' or guessing attacks.
- There are a number of additional considerations you will need to take account of when designing your password system, such as the use of an appropriate hashing algorithm to store your passwords, protecting the means by which users enter their passwords, defending against common attacks and the use of two-factor authentication.

In brief

- [What is this guidance about?](#)
- [What is required under the UK GDPR?](#)
- [What else do we need to do?](#)
- [What are the challenges in choosing the right authentication scheme?](#)
- [Are passwords the best choice?](#)
- [What makes a secure and useable password system?](#)
- [What should we consider when implementing a password system?](#)
- [How should we store passwords?](#)
- [How should our users enter their passwords?](#)
- [What requirements should we set for user passwords?](#)
- [What should we do about password expirations and resets?](#)
- [What defences can we put in place against attacks?](#)
- [What else do we need to consider?](#)

What is this guidance about?

This guidance is intended for use when you want to implement a password-based authentication scheme for an online service. It outlines the considerations that you should have where your authentication scheme will be protecting access to personal data.

Using passwords or other credentials for your internal network and information systems are out of scope of this guidance. However, there may be content that applies in this context all the same.

Before reading and applying this guidance, you should consider whether passwords are the most appropriate method of authenticating users, or whether other alternatives will provide more security and less friction for users.

What is required under the UK GDPR?

The UK GDPR does not say anything specific about passwords. However, Article 5(1)(f) states that personal data shall be:

“

‘Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’

This is the UK GDPR’s ‘integrity and confidentiality’ principle, or, more simply, the ‘security’ principle. So, although there are no provisions on passwords, the security principle requires you to take appropriate technical and organisational measures to prevent unauthorised processing of personal data you hold.

This means that when you are considering a password setup to protect access to a system that processes personal data, that setup must be ‘appropriate’.

Although the UK GDPR does not define what is ‘appropriate’, it does provide further considerations in Article 32, ‘security of processing’:

“

‘Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.’

This means that when considering any measures, you can consider the state of technological development and the cost of implementation – but the measures themselves must ensure a level of security appropriate to the nature of the data being protected and the harm that could be caused by unauthorised access.

In other words, you cannot simply set up a password system and then forget about it – there must be a periodic review process.

What else do we need to do?

You must ensure that you are aware of the state of technological development in this area and that your processes and technologies are robust against evolving threats.

For example, advances in processing power can reduce the effectiveness of cryptography or particular

design choices can become outdated.

You must also consider whether there might be better alternatives to passwords that can be used to secure a system.

Article 25 of the UK GDPR also requires you to adopt a data protection by design approach. This means that whenever you develop systems and services that are involved in your processing, you should ensure that you take account of data protection considerations at the initial design stage and throughout the lifecycle. This applies to any password system you intend to use.

At the same time, provided you properly implement a password system, it can be an element that can be used to demonstrate compliance with your obligations under data protection by design.

Further Reading

 Relevant provisions in the UK GDPR - See Articles 5(1)(f), 25, 32 and Recitals 39, 78 and 83 
External link

Further reading

- Security
- Data protection by design and by default
- ICO/NCSC security outcomes

What are the challenges in choosing the right authentication scheme?

One of the biggest challenges you face when dealing with personal data online is ensuring that such data can be accessed only by those with the correct permissions - in other words, authenticating, and authorising, the individual who is trying to gain access.

It is commonly accepted that there are three main ways of authenticating people to a system – checking for:

- something the individual has (such as a smart card);
- something the individual is (this is usually a biometric measure, such as a fingerprint); or
- something the individual knows.

Of these, the most commonly used is something the individual knows. In most cases something they know is taken to be a password.

Passwords remain the most popular way that individuals authenticate to online services. The reason for this is that a password is generally the simplest method to deploy and the most familiar for individuals.

Despite this, passwords carry well-known risks. The biggest risk is that people passwords as a mathematical problem that can be solved by increasing complexity rules. This fails to take into account

natural human behaviour which is to make passwords more easily memorable, regardless of the cost to security.

A rigid focus on password strength rules with no consideration of the usual behaviour of people choosing passwords means that you can make inappropriate choices in setting up and maintaining of your authentication system. This could place the wider security of your systems or your users at risk, and could lead to unauthorised or unlawful access to personal data.

Are passwords the best choice?

The success of using a password to properly authenticate a user of your service relies on the fact that their password remains a shared secret between you and them. When a password is shared amongst users or can be easily guessed by an attacker it can become extremely difficult to tell the difference between an authorised user and an imposter with stolen or guessed credentials.

The proliferation of online services requiring individuals to create an account has created a risk that people become overwhelmed with access credentials and default to reusing a short and memorable password (often coupled with the same email address as a username) across multiple websites.

The risk here is that if one service suffers a personal data breach and access credentials are compromised, these can be tested against other online services to gain access – a technique known as ‘credential stuffing’.

Example

In 2012, the social networking site LinkedIn was hacked. It was thought at the time that passwords for around 6.5 million user accounts were stolen by cybercriminals. However, in May 2016, following the advertisement for sale on the dark web of 165 million user accounts and passwords, [LinkedIn confirmed that the 2012 attack had actually resulted in the theft of email addresses and hashed passwords of approximately 165 million users](#).

The vast majority of the passwords were subsequently cracked and posted online less than a day after the further distribution, largely due to the use of SHA1 without a salt as the hashing algorithm. Due to the reuse of passwords across online services, a number of subsequent account takeovers at other services were attributed to the LinkedIn hack.

Before designing and implementing a new password system, you should consider whether it is necessary to do so, or whether there is a better alternative that can provide secure access.

One common alternative to building your own solution is to utilise a single sign on (SSO) system. While this has its advantages (not least a reduction in the number of passwords that a user has to remember) you must ensure that you are happy with the level of security that is offered by that system. You should ensure that you have a documented record of the considerations you made when reaching this decision.

You must also consider what will happen if the SSO is compromised, as this will most likely result in your user’s accounts also being compromised.

What makes a secure and useable password system?

A good password system is one that provides you with sufficient assurance that the individual attempting to log in is the user they claim to be. In practice, this means a good password system should protect against two types of attack:

- firstly, it should be as difficult as possible for attackers to access stored passwords in a useable form; and
- secondly, it should protect against attackers trying to brute force or guess a valid password and username combination.

Your system should also make it as easy as possible for users to create secure and unique passwords that they can remember or store easily. It should not place an undue burden on individuals to make sure that their account is secure. Putting such barriers in place can result in users making less secure password choices.

The advice provided in this guidance is a good starting point for most systems where personal data is being protected. It will be updated as necessary, but you should consider whether you need to apply a higher level of security given your particular circumstances.

This will largely depend on the nature, scope, context and purposes of your processing and the risks it poses. However, in essence, the more serious the consequences of a compromise, the higher the level of security that you will require.

You should ensure that you stay up to date with the current capabilities of attackers who might try to compromise password systems. You should also consider advice from other sources, such as the [National Cyber Security Centre](#) (NCSC) and GetSafeOnline.

Other resources

Guidance on passwords from the NCSC:

- [NCSC passwords guidance collection](#)
- [Passwords: updating your approach ↗](#)
- [Using passwords to protect your data from the NCSC small business guide](#)

Guidance on passwords from GetSafeOnline:

- [Password protocol and control ↗](#)

Guidance on avoiding credential stuffing attacks from the Global Privacy Assembly:

- [Awareness raising for individuals ↗](#)
- [Guidelines for organisations ↗](#)

What should we consider when implementing a password system?

If you are going to put in place a password system, you should take account of factors like:

- how you will process user passwords;
- how your users enter their passwords;
- the requirements you set for user passwords;
- what you do about password expirations and resets;
- the defences you put in place against attacks; and
- any additional considerations.

How should we store passwords?

Do not store passwords in plaintext - make sure you use a suitable hashing algorithm, or another mechanism that offers an equivalent level of protection against an attacker deriving the original password.

Well-known hashing algorithms such as MD5 and SHA1 are not suitable for hashing passwords. Both algorithms have known security weaknesses which can be exploited, and you should not use these for password protection in any circumstances. The biggest weakness with these algorithms is the speed that hashes can be calculated.

You should also consider avoiding other fast algorithms. Use a hashing algorithm that has been specifically designed for passwords, such as bcrypt, scrypt or PBKDF2, with a salt of appropriate length.

It is important that you review the hashing algorithms you use, as over time they can become outdated. Guidance on algorithms is available from a number of organisations such as [the NCSC](#), the [National Institute of Standards in Technology](#) (NIST) and the [European Union Agency for Cybersecurity](#) (ENISA). You should also be aware of any sector-specific guidelines that are available and may be applicable to you.

You should make sure that you can replace any algorithm that becomes obsolete.

You should also ensure that the architecture around your password system does not allow for any inadvertent leaking of passwords in plaintext.

Example

In 2018, Twitter and GitHub discovered that errors in their logging systems had led to plaintext passwords for users being stored in log files. Although the log files were not exposed to anyone outside of the organisations, both Twitter and GitHub recommended or required that users changed their passwords.

Other resources

Information on the status of a number of hashing functions can be found in NIST Special Publication 800-131A Revision 2 – [Transitioning the use of cryptographic algorithms and key lengths](#) (2019) (PDF)

ECRYPT-CSA's 2018 '[Algorithms, key size and protocols](#)' report (external link, PDF) provides further information on the status of cryptographic hash functions.

How should our users enter their passwords?

You should ensure that your login pages are protected with HTTPS, or some other equivalent level of protection. Failure to do so will mean that anyone who is in a position to intercept network traffic can obtain passwords and may be able to carry out replay attacks. You should also consider that browsers now mark pages that require secure input (such as login pages) as insecure if they are delivered over HTTP, and many browsers now mark all pages delivered over HTTP as insecure.

Further reading

Section on [data transfer](#) from our guidance on [encryption](#).

Make sure that password hashing is carried out server-side, rather than client-side. Hashing client-side will remove the protection afforded by hashing in the first place, unless other mitigations are put in place. This is a complicated area with a number of factors to consider. At the most basic level, if you are hashing client-side and an attacker obtains your password database, then those hashes can be presented directly to the server for a successful login.

Also, you should not prevent users from pasting passwords into the password field. Preventing pasting is often seen as a security measure, but at the same time doing so can impede people from using password managers effectively. The NCSC's position on password pasting is the same, as expressed in this [blog post](#) discussing this issue in much more detail. Any attacks that are facilitated by allowing pasting can be defended against with proper rate limiting (see [below for more details on rate limiting](#)).

Other resources

Read the NCSC's '[Let them paste passwords](#)' blog post for more information on why you should allow your users to paste passwords into password fields.

What requirements should we set for user passwords?

There are three general requirements for any password system that you will need to consider:

- password length - you should set a suitable minimum password length (this should be no less than 10 characters), but not a maximum length. If you are correctly hashing your passwords, then the output

should be the same length for every password, and therefore the only limit to password length should be the way your website is coded. If you absolutely must set a maximum length due to the limitations of your website code, then tell users what it is before they try to enter a password. The reasoning behind having a maximum length should be documented and fully risk assessed;

- special characters - you should allow the use of special characters, but don't mandate it. If you must disallow special characters (or spaces) make sure this is made clear before the user creates their password; and
- password 'deny lists' - do not allow your users to use a common, weak password. Screen passwords against a password 'deny list' of the most commonly used passwords, leaked passwords from website breaches and common words or phrases that relate to the service. Update this list at least yearly. Explain to users that this is what you are doing, and that this is why a password has been rejected.

Example

A password 'deny list' could be a feature of the software you use. Other lists are available online, e.g. [SecLists](#) and [haveibeenpwned's](#) password list.

It is also possible to find easy implementations, such as [NIST Bad Passwords](#), which uses SecLists.

Other than the three requirements listed above, do not set restrictions on how users should create a password. Research (see 'Other resources' below) indicates that doing so will cause people to reuse passwords across accounts, to create weak passwords with obvious substitutions or to forget their passwords. All this places unnecessary stress on your reset process and weakens the overall security of your service.

Properly set up and configured password strength meters can be a good way to easily communicate the requirements listed above to your users, and research has shown that good meters can assist users in choosing strong passwords. If you decide to use one, make sure it properly reflects what constitutes a strong or weak password.

Other resources

Microsoft's [password guidance](#) (PDF) (external link) contains advice on passwords in the context of several Microsoft platforms. It includes guidance for IT administrators as well as users, and details a number of common password attacks and highlights a number of issues including the risks of placing restrictions on how users create passwords.

Advice from [the Federal Trade Commission](#) (FTC) (external link) also discusses these issues.

For more information on password strength meters, read [this analysis](#) (external link) from Sophos as well as the [significant amount of research](#) (external link) from Carnegie Mellon University.

Finally, remind your users that they should not reuse passwords from other services. In most circumstances you should not know what your user's passwords are. However, some companies actively track compromised credentials that are traded on the dark web and will check these credentials against the hashes they hold on their systems to see if there is a match.

If you decide that this is something you want to do you need to carefully consider the potential legal implications of obtaining such lists, and you will need to explain very clearly how you use that data to your users (especially where the use of such data has led to a password reset or an account lockout).

If users receive an email asking them to reset their password without a proper explanation they will generally assume that the problem is with your service, so it is in your interests to explain precisely why you are taking this action.

What should we do about password expirations and resets?

You should only set password expirations if they are absolutely necessary for your particular circumstances. Regular expiry often causes people to change a single strong password for a series of weak passwords.

As a general rule, get your users to create a strong initial password and only change them if there are pressing reasons, such as a breach of your systems that may have resulted in the password hashes being compromised, or if you receive some other indication that a user's password may have been compromised.

When deploying a password reset process you should ensure that it is secure. Do not send passwords over email, even if they are temporary – use one time links, and ensure that you do not leak the credentials in any referral headers.

You should also not be in a position where a member of your staff is able to 'read out' a user's password to them, eg over the phone in a service call—this indicates that you are storing passwords in plaintext, which is, as described above, not appropriate. If you require a password to validate a user over the phone, set a separate phone password for the account.

You should also time limit any password reset credentials. The majority of users will probably reset their password immediately, but set a limit that fits your observed user behaviour.

Other resources

Read the FTC's [advice about the potential issues with mandatory password changes](#) from 2016 (external link).

What defences can we put in place against attacks?

Ensure that you are rate limiting or 'throttling' the number and frequency of incorrect login attempts. The precise number of attempts and the consequence of exceeding these limits will be for you to decide based on the specific circumstances of your organisation, but limiting to a certain number per hour, day and month is a good idea.

This will help to deter both bulk attackers and people targeting individual accounts.

Example

[NIST guidance](#) recommends that accounts with internet access should be limited to 100 consecutive failed attempts on a single account unless otherwise specified in the system being deployed.

There are additional considerations when implementing your rate limits:

- you should be aware that some attackers will deliberately work within your limits to avoid detection, and will still achieve a reasonable success rate, especially with targeted guessing;
- set your limits based on observed behaviour of both attackers and your users;
- be aware that overly-aggressive rate limiting can be used as a denial of service attack (remember that the UK GDPR requires the availability of personal data); and
- remember that a number of successful or unsuccessful access attempts to a range of different user accounts from the same device or IP address might be indicative of a bulk attack.

You should also consider whether other methods of preventing attacks might be appropriate. Examples of these methods could include, but are not limited to:

- the use of 'CAPTCHAs';
- creating an 'allow list' of IP addresses; and
- time limits or time delays after failed authentications.

What else do we need to consider?

You need to address how your system will respond to an attacker who has legitimate credentials for a user, or for multiple users. There is a distinct possibility that you will encounter this scenario given that both password reuse and website breaches are relatively common occurrences.

Techniques for recognising common user behaviour are becoming more advanced, and you could use these to develop a risk-based approach to verifying an authentication attempt. For example, if a user logs in from a new device or IP address you might consider requesting a second authentication factor and informing the user by another contact method of the login attempt.

It is however important to remember that collecting additional data from users in order to defend against authentication attacks could itself constitute processing personal data and should operate in compliance with the UK GDPR. This does not mean you cannot process this data, but you must ensure that you have considered the data protection implications of doing so.

You should consider providing your users with the facility to review a list of unsuccessful login attempts. This will allow people who might be specifically targeted to check for potential attacks manually. However, this will only be useful if you pay attention to reports from individuals that their accounts are being attacked.

You should implement two-factor or multifactor authentication wherever it is possible to do so - to take the most common example, a password and a one-time token generator. This will be more important where the

personal data that can be accessed is of a sensitive nature, or could cause significant harm if it were compromised.

Other examples of a second factor that could be used include biometrics (fingerprints being the most common and easy to implement), smart cards or U2F keys and devices.

You will however need to ensure that any processing of biometric data for the purposes of uniquely identifying an individual is done in accordance with the requirements for processing special category data in both the UK GDPR and the Data Protection Act 2018.

Further reading

[Key definitions](#) section of the Guide to the UK GDPR

Other resources

Additional guidance on digital identities, hashing functions and algorithms and passwords in general includes:

- NIST's Special Publication 800-63 on digital identity guidelines [↗](#) (external link);
- NIST's policy on hashing functions [↗](#) (external link);
- ECRYPT-CSA's 2018 report into 'Algorithms, key size and protocols [↗](#)' (external link, PDF);
- The International Working Group on Data Protection in Telecommunications (the 'Berlin Group') [Working Paper on biometrics in online authentication ↗](#) in 2016 (PDF) (external link);
- OWASP cheat sheet on password storage [↗](#) (external link);
- The NCSC's password guidance (external link);
- Additional NCSC guidance on the use of multi-factor authentication in online services [↗](#) (external link). Although primarily aimed at large organisations, this guidance summarises the considerations involved in implementing an 'extra factor' for authentication, including the options for those factors; and
- Cynosure Prime's analysis of 320 million leaked passwords from the HaveIBeenPwned website [↗](#) (external link)

Ransomware and data protection compliance

At a glance

- Personal data breaches from the ICO's caseload during 2020/2021 have seen a steady increase in the number and severity caused by ransomware. This is a type of malicious software or "malware" designed to block access to computer systems, and the data held within them, using encryption.
- Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.
- This guidance presents eight scenarios about the most common ransomware compliance issues we have seen.

Checklist

Governance

- We establish and communicate a set of suitable security policies that provide direction to appropriate levels of security.

Asset identification

- We identify, document and classify the personal data we process and the assets that process it. Examples of personal data that typically require a higher classification level include large volumes of data, children's data and special category data.

Technical control selection

- We determine and document appropriate controls to protect the personal data we process. We use the [NCSC Mitigating Malware and Ransomware guidance](#) to give us a set of practical controls we can implement to prevent ransomware.

Access controls

- We implement appropriately strong access controls for systems that process personal data. For internet facing services, such as remote access solutions, we enable multi-factor authentication or other alternatively strong access controls.

Vulnerability management

- We implement a policy that defines our approach to patch management. We prioritise patches relating to internet-facing services, as well as critical and high risk patches. We use the [NCSC Vulnerability management guidance](#) to support us further.

Staff education and awareness

- We ensure all relevant staff have a baseline awareness of attacks such as phishing. We consider providing additional and specific security training for staff with responsibility for IT Infrastructure and security services.

Detection

- We implement appropriate controls to be able to detect and respond to an attack before it can exploit the personal data we process. If we are a smaller organisations, we use the [NCSC Logging Made Easy](#) solution to support us in developing basic enterprise logging capability.

Incident response

- We define an incident response plan that guides us in the event of a ransomware attack. We include thresholds for ICO and affected individual notifications.
- We perform regular tests of our plan, for example, the [NCSC Exercise in a Box](#) helps us practise our response in a safe environment.

Disaster recovery

- We have disaster recovery and business continuity plans to support us in restoring personal data in a timely manner. Measures such as offline backups or those described in the [NCSC "Offline backups in an online world" blog](#) are important to ensure we can restore personal data.

Assurance

- We test, assess and evaluate our control environment using measures such as audits, vulnerability scanning, penetration testing and accreditation against proven security standards such as [NCSC Cyber Essentials](#) and other relevant standards of good practice.

In brief

- [What is ransomware?](#)
- [Why is ransomware an important data protection topic?](#)
- [What can we do to prevent ransomware?](#)
 - [Scenario 1: Attacker sophistication](#)
 - [Scenario 2: Personal data breach](#)
 - [Scenario 3: Breach notification](#)
 - [Scenario 4: Law enforcement](#)
 - [Scenario 5: Attacker tactics, techniques and procedures](#)
 - [Scenario 6: Disaster recovery](#)
 - [Scenario 7: Ransomware payment](#)
 - [Scenario 8: Testing and assessing security controls](#)

What is ransomware?

Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.

A ransomware attack occurs when an attacker gains access to an organisation's computer systems and delivers malicious software into the network. This software, or 'payload,' then makes the data unavailable through encryption or deletion. Ransomware is often designed to spread from device to device to maximise the number of files it can encrypt.

The 'ransom' element comes from the ransom note left by the attacker requesting payment in return for restoring the data. This is usually done by a decryption key that only the attacker can access.

Where personal data is encrypted as the result of a ransomware attack, that constitutes a personal data breach because you have lost timely access to the data.

Unless you have a backup of the data, you will not usually be able to recover it unless you decide to comply with the attacker's demand for payment. Even if you decide to pay the ransom fee, there is no guarantee that the attacker will supply the key to allow you to decrypt the files.

Why is ransomware an important data protection topic?

In recent years, ransomware attacks are one of the most common cyber incidents affecting personal data. The attack can lead to the loss of timely access to personal data. Permanent data loss can also occur, if appropriate backups are not in place.

The National Cyber Security Centre (NCSC) recognises ransomware as the biggest cyber threat facing the United Kingdom. The most recent threat landscape report from the European Union Agency for Cyber Security (ENISA) has also assessed ransomware as the prime threat with cybercriminals increasingly motivated by monetisation.

The attacks are becoming increasingly damaging and this trend is likely to continue. Malicious and criminal actors are finding new ways to pressure organisations to pay. For example, through uploading a copy of your data and threatening to publish it.

As criminal actors look for additional ways to exploit the captured data, the risks to individuals have increased, including:

- potential permanent personal data loss;
- potential loss of control over their personal data;
- being further targeted in social engineering style attacks using the breached data (eg phishing emails); and
- their personal data being further maliciously used by criminal actors (eg to facilitate identify and financial fraud).

Sectors such as education, health, legal services and business are amongst the most targeted. However, all UK businesses that process personal data are at risk. This is due to the low barriers to entry, such as by using ransomware-as-a-service and opportunistic attacks.

What can we do to prevent ransomware?

You should review our checklist above, as well as the following eight scenarios. These are the eight most common ransomware compliance issues we have identified, based on past personal data breaches.

Scenario 1: Attacker sophistication

I am a small organisation that is aware of the growing threat of ransomware. However, I don't think attackers will be interested in targeting me. If they do, how can I protect the personal data I process?

'Scatter gun' style attacks are a common attack method. This is a type of attack that is indiscriminate and does not have a specific target. For example, the attacker may send thousands of phishing emails attempting to deliver ransomware to at least one victim, whoever that may be.

The [NCSC Cyber Essentials ↗](#) is designed to support you in preventing basic and common types of attacks. The measures they describe will help you apply appropriate security measures, which are a requirement of the UK GDPR.

For medium and larger organisations, maintaining good cyber security practices is essential to defend against ransomware attacks. Assessing your cyber security arrangements and capabilities against relevant good practice models can support you protect personal data from the threat of ransomware, such as:

- [NCSC 10 Steps to Cyber Security; ↗](#)
- [ISO27001 for Information Security ↗](#); and
- [NIST Cyber Security Framework ↗](#).

The [NCSC Mitigating Malware and Ransomware attacks ↗](#) also provides specific guidance that can support you in preventing such attacks.

Scenario 2: Personal data breach

We have been subjected to a ransomware attack, but personal data has not been uploaded from our systems to the attacker. If the data has not been removed does this mean a personal data breach has not occurred?

If you are subject to a cyber-attack, such as ransomware, you are responsible for determining if the incident has led to a personal data breach. This is your first step in deciding if you should notify the ICO about the incident.

The UK GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Where personal data is taken it typically results in unauthorised disclosure or access to personal data and therefore is a type of personal data breach. However, it is not the only consideration you should make when determining if a personal data breach has occurred.

You may have lost timely access to the personal data, for example because the data has been encrypted. This is a type of personal data breach because you have lost “access to” personal data. Temporary loss of access is also a type of personal data breach. For example, if there is a period of time before you restore from backup.

Therefore, loss of access to personal data is as much of a personal data breach as a loss of confidentiality.

However, just because a personal data breach has occurred does not automatically mean you should notify the ICO. Scenario 3 deals with a common breach notification scenario.

Scenario 3: Breach notification

We have established a personal data breach has occurred, but data has not been exfiltrated, therefore there are no risk to individuals. Do we still need to notify the ICO?

You are required to notify the ICO of a personal data breach without undue delay and no later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

This means once you have established a personal data breach has occurred, you should undertake a formal risk assessment. This is to determine the risks to individuals and the likelihood of such risks occurring. If you determine the risks to be unlikely, you do not need to notify the ICO. However, you must keep a record of any personal data breaches, regardless of whether you are required to notify, together with the risk assessment undertaken.

Where data is uploaded from your systems to the attacker it can increase the risks to individuals. Therefore, you should take data exfiltration into account as part of your risk considerations. Appropriate logging can support you in determining if personal data is likely to have been exfiltrated. The NCSC blog post [“What exactly should we be logging”](#) can support you in deciding what logs to collect and retain.

Without appropriate logs you may not generate the evidence to allow you to make an informed decision. If you determine there is no evidence of data exfiltration, the ICO may ask you to demonstrate what logs and measures you used to make this decision.

However, whilst exfiltration is an important consideration it is not the only one you should make. You should consider the rights and freedoms of individuals in totality. For example:

- Does the lack of availability impact on any individual rights, such as right of access to the personal data?
- Have individuals lost control of their personal data?
- Can you restore the personal data in a timely manner? If not, what does this mean for individuals?
- To what degree was the personal data exposed to unauthorised actors and what are their likely motivations?
- How confident are you in your detection and monitoring controls – could you have detected personal data being uploaded if it had occurred? If you do not have appropriate logs to make an informed decision, it may be helpful to determine if the attacker had the means, motivation and opportunity to

exfiltrate the data. You can then use this assessment to make a risk-based decision.

Further reading

The ICO's [Personal data breach assessment tool](#) can support you in identifying reportable personal data breaches.

Our [guidance on personal data breaches](#) can also further support you in assessing reportable personal data breaches.

Scenario 4: Law enforcement

A ransomware attack has breached the personal data we process. We are planning to notify individuals, however, law enforcement are currently collecting evidence as this was a criminal attack. They have requested we delay notifying individuals until they have completed this. How do I comply with my GDPR obligations whilst also cooperating with law enforcement?

If you have been subjected to a ransomware attack it is recommended you should contact law enforcement.

Law enforcement play a fundamental role in protecting individuals and the ICO work closely with these agencies in providing a multi-agency response to ransomware. Recitals 86 and 88 of the UK GDPR provide direction should law enforcement recommend delaying data subject notification:

Recital 86:

“

Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities

Recital 88:

“

Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach

However, law enforcement involvement does not automatically mean you should delay notifying individuals. Should law enforcement request a delay in a public notification, you should work closely with the ICO. This will allow us to work with you and law enforcement to assess the risk to the individuals under respective legislation.

Scenario 5: Attacker tactics, techniques and procedures

We have recently seen an increase in phishing emails coming into our organisation and are looking at what measures we can put in place to mitigate this risk. Are there any other specific attacker tactics that the ICO commonly see in ransomware attacks?

Tactics, techniques and procedures (TTPs) describe the methods attackers use to compromise data. Different attacks will use different types of TTPs, for example phishing is a common TTP to trick someone into giving up their credentials.

However, attacker TTPs are constantly evolving, as described within scenario one of this report. A good baseline of controls will reduce the likelihood of being exploited by basic levels of attack, such as those described in the NCSC Cyber Essentials.

Frameworks are available, such as the [Mitre ATT&CK](#) that provide a knowledgebase of TTP based on real world observations. The framework outlines each stage of an attack and the common TTPs that are used. These are a great resource to support you in identifying if your controls are appropriate to resist known TTPs.

During 2020/2021, we identified four of the most common TTPs from ransomware casework. The following practical advice for each example will support you in implementing appropriate measures.

Phishing: Attackers typically use social engineering techniques to trick you into doing something. Phishing is a common method we've seen to either deliver ransomware by email or to trick you into revealing your username and password.

Your security strategy should include ensuring all relevant staff receive basic awareness training in identifying social engineering attacks. In addition, you should consider tailoring the measures in the [NCSC Phishing Attack guidance](#) to your own organisation.

Remote access: The most common entry point into a network was by the exploitation of remote access solutions. Attackers often scan the internet for open ports such as remote desktop protocol and use this as an initial entry point. If they can capture valid credentials (eg by phishing, password database dumps or password guessing through brute force), they can authenticate by the remote access solution.

You should risk assess and document your remote access solution and identify appropriate measures in response to the risks. An access control policy that directs you to the minimum levels of controls required will support you in applying appropriate measures.

You should not use single-factor authentication on internet facing services, such as remote access, if it can lead to access to personal data. Use multi-factor authentication, or other comparably secure access

controls.

The [NCSC device security guidance](#) provides further advice on designing a remote access architecture for enterprise services.

Privileged account compromise: Once an attacker has a foothold in the network it is common that they compromise a privileged account, such as a domain administrator account. This is typically done by either

- compromising weak passwords of privileged accounts;
- compromising service accounts that do not belong to a particular user;
- using well known tools to extract plain text domain administrator passwords, password hashes or Kerberos tickets from the host; or
- exploiting a known software or application vulnerability which has a patch available to fix it.

Once an attacker can elevate their privileges to a domain administrative level account they are typically in a commanding position and will usually deploy the ransomware through the domain controller.

The security of privileged accounts should be a high priority for you. Basic account hygiene can support you in protecting these accounts, such as:

- regular reviews of permissions;
- following the principle of least privilege;
- risk assessments of membership into privileged groups; and
- senior level approval of privileged group membership.

Further reading

The NCSC has a selection of guidance available that can further support you in identifying appropriate measures to protect privileged accounts.

- [How to do secure system administration](#)
- [Protecting system administration with PAM](#)

Known software or application vulnerabilities: The exploitation of known vulnerabilities where patches were available to fix the issue is a common method used by attackers. This was much more common than zero-day attacks where the vulnerability exploited is not yet publicly known and is typically crafted by advanced levels of attackers. In particular, attackers often scan, sometimes indiscriminately, for known vulnerabilities present in internet-facing device and services.

The [NCSC vulnerability management guidance](#) will support you in managing vulnerabilities within your estate.

Considering the following will also support you in managing known vulnerabilities:

- Identify the assets within your organisation, including the software and application you use.
- Define and direct your approach to the patch management lifecycle, including the process of identifying, assessing, acquiring, testing, deploying and validating patches.
- Maintain software and applications that are in support by the vendor.

- Identify vulnerabilities within your estate for both internal and external hardware and software (eg vulnerability scanning).

Scenario 6: Disaster recovery

We understand the UK GDPR requires appropriate controls to be able to restore personal data in the event of a disaster. We currently backup our data so we are able to restore it in the event of a ransomware attack. Is there anything else we should consider?

A ransomware attack can be amongst the most stressful times for an organisation. Planning for such an event is critical in ensuring you have the measures in place to be able to appropriately respond to it.

For smaller and medium sized organisations the [NCSC Small Business Guide Response and Recovery ↗](#) gives you practical advice that will help you plan for dealing with an incident such as a ransomware attack.

For larger organisations the [NCSC Incident Management guidance within its 10 steps to cyber security ↗](#) can support you in implementing appropriate controls.

A backup of your personal data is one of the most important controls in mitigating the risk of ransomware. However, it is common that attackers will attempt to either delete or encrypt your backup. You should therefore consider if your current backup strategy could be at risk. Performing a threat analysis against your backup solution and considering how an attacker could delete or encrypt the data is recommended. The questions below will help you get started in your threat assessment:

- Is your backup segregated or offline?
- What would an attacker need to compromise to gain access to the backup? For example, what accounts can access the backup? What accounts can perform deletion or edit the backups? How could an attacker compromise these accounts? How do you protect accounts that can access the backups?
- Are you able to detect changes to your backup? For example, if an attacker initiated a deletion of your backup, could you detect this?
- What device or IP address or both can access the backup repository? Can this be spoofed? Can an attacker access the device or repository that stores the backup?
- How would you respond if an attacker deleted or encrypted your backup?

Using your threat analyses will help you identify controls to mitigate the risks. Offline backups that are completely offline from the main network are one of the most secure ways to prevent attackers from accessing it. If you are using cloud backups, you should read the NCSC blog posts about protecting these backups [Offline Backups in on online world ↗](#) and [Cloud Backup options for mitigating the risk of ransomware ↗](#).

Scenario 7: Ransomware payment

The attacker has provided a ransomware note saying it can restore the data if we pay the ransom fee. The attacker has also stated that if we pay they will not publish the data, so we are also considering if this would further reduce risk to individuals.

Does the ICO recommend the payment of the ransom to restore the data and mitigate risks to individuals?

Before paying the ransom, you should take into account that you are dealing with criminal and malicious actors. Even if you pay, there is no guarantee that they will provide you with the decryption key. "Double extortion" is also common, where you pay for the decryption key and the attacker then requires an additional payment to stop the publication of the data. Attack groups may also target you again in the future if you have shown willingness to pay.

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. The ICO supports this position.

You should also consider the terminology within the UK GDPR. It requires you to implement "appropriate measures" to restore the data in the event of a disaster. The ICO does not consider the payment of a ransom as an "appropriate measure" to restore personal data.

Appropriate measures include threat assessments, risk assessments and controls such as offline and segregated backups. If you can demonstrate appropriate measures in accordance with the state of the art, cost and risk of processing then you will be able to demonstrate "appropriate measures" and comply with those aspects of the UK GDPR.

If attackers have exfiltrated the personal data, then you have effectively lost control over that data. This means individuals have lost the protections and rights provided by the UK GDPR. For example, transparency of processing or subject access rights. For this reason, we do not view the payment of the ransom as an effective mitigation measure.

If you do decide to pay the ransom to avoid the data being published, you should still presume that the data is compromised and take actions accordingly. For example, the attacker may still decide to publish the data, share the data offline with other attack groups or further exploit it for their own gains. You still need to consider how you will mitigate the risks to individuals even though you have paid the ransom fee.

Scenario 8: Testing and assessing security controls

I want to protect my organisation and the personal data I process from ransomware. Is there any type of testing I can do to assess whether my controls are appropriate?

The UK GDPR requires you to regularly test, assess and evaluate the effectiveness of your technical and organisational controls using appropriate measures. There is no one test that you can carry out, you should consider this within your wider security framework.

For the examples discussed within this review, we have provided several suggested methods which will

support you in adopting appropriate measures:

- **Breach notification:** Document and perform regular tests of your incident response plan so you are prepared for a real incident. The [NCSC Exercise in a Box](#) tool can help you practice your incident response in a safe environment.
- **Account management:** Regularly audit your user accounts to ensure they are still required and contain the appropriate privileges. This should include reviews to ensure staff have not retained privileges from previous internal job roles that are no longer required, often called “privilege creep”. Ensure you document such reviews. Consider controls to identify weak or previously breached passwords.
- **Patch management:** Have a method to identify vulnerabilities in your network, such as missing patches. Vulnerability scans are an effective tool that can support this.
- **Attack tactics, techniques and procedure:** Risk assess and document your security controls to determine if they are appropriate to resist known TTPs. Penetration testers often simulate attacker activity by applying TTPs to vulnerabilities within your environment.
- **Audit:** Perform and record regular audits of your environment against a proven security standard, such as Cyber essentials (for smaller organisations) or ISO27001 (for medium and larger organisations).
- **Disaster recovery:** Perform and record regular tests of your disaster recovery plan to ensure it is effective. For example, perform a restore of personal data to ensure the data can be restored within the recovery time objective.

As with any tests, reviews, and assessments, ensure you document and appropriately retain these records, as you may need to submit them to the ICO.

Encryption

At a glance

- The UK GDPR requires you to implement appropriate technical and organisational measures to ensure you process personal data securely.
- Article 32 of the UK GDPR includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities.
- Encryption is a widely-available measure with relatively low costs of implementation. There is a large variety of solutions available.
- You should have an encryption policy in place that governs how and when you implement encryption, and you should also train your staff in the use and importance of encryption.
- When storing or transmitting personal data, you should use encryption and ensure that your encryption solution meets current standards.
You should be aware of the residual risks of encryption, and have steps in place to address these.

Checklists

- We understand that encryption can be an appropriate technical measure to ensure that we process personal data securely.
- We have an appropriate policy in place governing our use of encryption.
- We ensure that we educate our staff on the use and importance of encryption.
- We have assessed the nature and scope of our processing activities and have implemented encryption solution(s) to protect the personal data we store and/or transmit.
- We understand the residual risks that remain, even after we have implemented our encryption solution(s).
- Our encryption solution(s) meet current standards such as FIPS 140-2 and FIPS 197.
- We ensure that we keep our encryption solution(s) under review in the light of technological developments.
- We have considered the types of processing we undertake, and whether encryption can be used in this processing.

In brief

- [What does the UK GDPR say about encryption?](#)

- What is encryption?
- Encryption and data storage
- Encryption and data transfer
- What types of encryption are there?
- How should we implement encryption?
- Encryption scenarios
- In detail

What does the UK GDPR say about encryption?

- The UK GDPR's security principle requires you to put in place appropriate technical and organisational measures to ensure you process personal data securely.
- Article 32 provides further considerations for the security of your processing. This includes specifying encryption as an example of an appropriate technical measure, depending on the risks involved and the specific circumstances of your processing. The ICO has seen numerous incidents of personal data being subject to unauthorised or unlawful processing, loss, damage or destruction. In many cases, the damage and distress caused by these incidents may have been reduced or even avoided had the personal data been encrypted.
- It is also the case that encryption solutions are widely available and can be deployed at relatively low cost.
- It is possible that, where data is lost or destroyed and it was not encrypted, regulatory action may be pursued (depending on the context of each incident).

What is encryption?

- Encryption is a mathematical function that encodes data in such a way that only authorised users can access it.
- It is a way of safeguarding against unauthorised or unlawful processing of personal data, and is one way in which you can demonstrate compliance with the security principle.
- Encryption protects information stored on mobile and static devices and in transmission, and there are a number of different encryption options available.
- You should consider encryption alongside other technical and organisational measures, taking into account the benefits it can offer and the risks it can pose.
- You should have a policy in place governing the use of encryption, including appropriate staff education.
- You should also be aware of any sector-specific guidance that applies to you, as this may require you to use encryption.

Encryption and data storage

- Encrypting data whilst it is being stored provides effective protection against unauthorised or unlawful processing.
- Most modern operating systems have full-disk encryption built-in.
- You can also encrypt individual files or create encrypted containers.

- Some applications and databases can be configured to store data in encrypted form.
- Storing encrypted data still poses residual risks. You will need to address these depending on the context of your processing, such as by means of an organisational policy and staff training

Encryption and data transfer

- Encrypting personal data whilst it is being transferred provides effective protection against interception by a third party.
You should use encrypted communications channels when transmitting any personal data over an untrusted network.
- You can encrypt data prior to transmission over an insecure channel and ensure it is still protected. However, a secure channel provides assurance that the content cannot be understood if it is intercepted. Without additional encryption methods, such as encrypting the data itself prior to transmission, the data will only be encrypted whilst in transit.
- You should look to use HTTPS across your entire site. While there are some circumstances that can make this difficult you still need to take appropriate steps such as ensuring that all areas of user input are protected.
- Encrypted data transfer still poses residual risks. You will need to address these depending on the context, such as by means of an organisational policy and staff training.

What types of encryption are there?

- The two types of encryption in widespread use today are symmetric and asymmetric encryption.
- With symmetric encryption, the same key is used for encryption and decryption. Conversely, with asymmetric encryption, different keys are used for encryption and decryption.
- When using symmetric encryption, it is critical to ensure that the key is transferred securely.
- The technique of cryptographic hashing is sometimes equated to encryption, but it is important to understand that encryption and hashing are not identical concepts, and are used for different purposes.

How should we implement encryption?

- When implementing encryption it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
- Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards such as FIPS 140-2 and FIPS 197.
- Advice on appropriate encryption solutions is available from a number of organisations, including the National Cyber Security Centre (NCSC).
- You should also ensure that you keep your keys secure, and have processes in place to generate new keys when necessary to do so.

Encryption scenarios

There are a number of typical data processing activities where you should consider the use of encryption. These are outlined in our detailed guidance which includes a section on common scenarios.

In each case, it is important that you consider the residual risks that remain even after you put the encryption in place.

Further reading

[Security](#)

[Security outcomes](#)

[Data protection by design and default](#)

We have published [detailed guidance on encryption](#) including a number of common scenarios and risks.

Personal data breaches

At a glance

- The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. 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. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

- We know how to recognise a personal data breach.
- We understand that a personal data breach isn't only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risk to individuals as a result of a breach.
- We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.
- We know we must inform affected individuals without undue delay.
- We know who is the relevant supervisory authority for our processing activities.

- We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We know what information we must give the ICO about a breach.
- We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- We document all breaches, even if they don't all need to be reported.

In brief

- [What is a personal data breach?](#)
- [Risk-assessing data breaches](#)
- [When do we need to tell individuals about a breach?](#)
- [What information must we provide to individuals when telling them about a breach?](#)
- [What breaches do we need to notify the ICO about?](#)
- [What role do processors have?](#)
- [How much time do we have to report a breach?](#)
- [What information must a breach notification to the ICO contain?](#)
- [What if we don't have all the required information available yet?](#)
- [How do we notify a breach to the ICO?](#)
- [Does the UK GDPR require us to take any other steps in response to a breach?](#)
- [What else should we take into account?](#)
- [What happens if we fail to notify the ICO of all notifiable breaches?](#)

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 includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;

- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Risk-assessing data breaches

Recital 87 of the UK GDPR says that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Remember, the focus of risk regarding breach reporting is on the potential negative consequences for individuals. Recital 85 of the UK GDPR explains that:

“

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, whose data may be used to commit identity fraud, would need to be notified, given its likely impact on those individuals who could suffer financial loss or other consequences. But you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

Example

- A hospital suffers a breach that results in accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.
- A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.
- A medical professional sends incorrect medical records to another professional. They inform the sender immediately and delete the information securely. This is unlikely to result in a risk to the rights and freedoms of the individual. They don't need to be informed about the breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of any data protection officer you have, 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 taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO, if reportable.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the UK GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft [UK GDPR guidance on contracts and liabilities between controllers and processors](#).

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details

of when a controller can be considered to have 'become aware' of a breach.

What information must a breach notification to the ICO contain?

When reporting a breach, the UK GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has 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 taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So its Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see our [pages on reporting a breach](#). These pages include a [self-assessment tool](#) and some [personal data breach examples](#).

Remember, a breach affecting individuals in EEA countries will engage the EU GDPR. This means that as

part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party [guidance on identifying your lead authority](#).

Does the UK GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts regarding the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the UK GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented. Human error is the leading cause of reported data breaches. To reduce the risk of this, consider:

- mandatory data protection induction and refresher training;
- support and supervising until employees are proficient in their role.
- updating policies and procedures for employees should feel able to report incidents of near misses;
- working to a principle of "check twice, send once";
- implementing a culture of trust – employees should feel able to report incidents of near misses;
- investigating the root causes of breaches and near misses; and
- protecting your employees and the personal data you are responsible for. This could include:
 - Restricting access and auditing systems, or
 - Implementing technical and organisational measures, eg disabling autofill.

As mentioned previously, as part of your breach management process you should undertake a risk assessment and have an appropriate risk assessment matrix to help you manage breaches on a day-to-day basis. This will help you to assess the impact of breaches and meet your reporting and recording requirements. This will provide a basis for your breach policy and help you demonstrate your accountability as a data controller.

What else should we take into account?

The following aren't specific UK GDPR requirements regarding breaches, but you should take them into account when you've experienced a breach.

As a result of a breach an organisation may experience a higher volume of data protection requests or complaints, particularly in relation to access requests and erasure. You should have a contingency plan in place to deal with the possibility of this. It is important that you continue to deal with those requests and complaints, alongside any other work that has been generated as a result of the breach. You should also consider how you might manage the impact to individuals, including explaining how they may pursue compensation should the situation warrant it.

It is important to be aware that you may have additional notification obligations under other laws if you

experience a personal data breach. For example:

- If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our [pages on PECR](#) for more details.
- If you are a UK trust service provider, you must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. You can use our [eIDAS breach notification form](#) or the GDPR breach-reporting process. However, if you report it to us under the UK GDPR, this still must be done within 24 hours. Please read our [Guide to eIDAS](#) for more information.
- If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the [NIS Directive](#). These are separate from personal data breach notification under the UK GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which has replaced the WP29, has endorsed the [WP29 Guidelines on Personal Data Breach Notification](#). Although the UK has left the EU, these guidelines continue to be relevant. You should also be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify the ICO of all notifiable breaches?

Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. It is important to make sure you have a robust breach-reporting process in place to ensure you detect, and notify breaches, on time and to provide the necessary details, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 33, 34, 58, 83 and Recitals 75, 85-88](#) 
External link

In more detail – ICO guidance

See the following sections of the Guide to the UK GDPR:

- Security
- Accountability and governance

GDPR 'in more detail' guidance:

International transfers after the UK exit from the EU Implementation Period

How have the rules on restricted transfers changed, now that the Brexit transition period has ended?

On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU's [General Data Protection Regulation](#) (EU GDPR) and [Law Enforcement Directive](#) (LED). In both cases, the European Commission has found the UK to be adequate. This means that most data can continue to flow from the EU and the EEA without the need for additional safeguards. The adequacy decisions do not cover data transferred to the UK for the purposes of immigration control, or where the UK immigration exemption applies. For this kind of data, different rules apply and the EEA sender needs to put other transfer safeguards in place.

This guidance is about transferring data overseas from the UK. For further information on receiving personal data from the EEA, read our detailed guidance on [data protection and the EU](#).

Restricted transfers from the UK to other countries, including to the EEA, are subject to transfer rules under the UK regime. These UK transfer rules broadly mirror the EU GDPR rules, but the UK has the independence to keep the framework under review.

There are transitional arrangements which aim to smooth the transition to the new UK regime.

First, there are provisions which permit the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision'. This is to be kept under review by the UK Government.

The UK government has the power to make its own 'adequacy decisions' in relation to third countries and international organisations. In the UK regime these are known as 'adequacy regulations'.

There are also provisions which allow the continued use of any [EU Standard Contractual Clauses](#) ('SCCs'), valid as at 31 December 2020, as long as the contract was entered into before 21 September 2022.

Finally, there are provisions which allow certain [Binding Corporate Rules](#) to transition into the UK regime.

Further Reading

[Data Protection and the EU](#)

For organisations

At a glance

- The UK GDPR primarily applies to controllers and processors located in the United Kingdom, with some exceptions.
- Individuals risk losing the protection of the UK data protection laws if their personal data is transferred outside of the UK.

- On that basis, the UK GDPR restricts transfers of personal data to a separate organisation located outside of the UK, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.
- We refer to a transfer of personal data to a separate organisation located outside of the UK as a “restricted transfer”.

Checklist

- 1. Are we planning to make a restricted transfer of personal data outside of the UK?**
If no, you can make the transfer. If yes go to Q2
- 2. Do we need to make a restricted transfer of personal data in order to meet our purposes?**
If no, you can make the transfer without any personal data. If yes go to Q3
- 3. Are there UK ‘adequacy regulations’ in relation to the country or territory where the receiver is located or a sector which covers the receiver (which currently includes countries in the EEA and countries, territories or sectors covered by existing EU ‘adequacy decisions’)?**
If yes, you can make the transfer. If no go to Q4
- 4. Are we putting in place one of the ‘appropriate safeguards’ referred to in the UK GDPR?**
If yes, go to Q5 If no go to Q6
- 5. Having undertaken a risk assessment, we are satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.**
If yes, you can make the transfer. If no, go to Q6.
- 6. Does an exception provided for in the UK GDPR apply?**
If yes, you can make the transfer. If no, you cannot make the transfer in accordance with the UK GDPR

If you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the UK GDPR.

Further Reading

The European Data Protection Board (EDPB) have published recommendations on measures that supplement transfer tools, for consultation. The recommendations (when finalised) will apply to the EU GDPR transfer regime, and are included here only as useful reference about additional measures. We will be producing our own guidance on this topic in due course.

In brief

- What are the restrictions on international transfers?
- Are we making a transfer of personal data outside the UK?
- Do we need to make a restricted transfer?
- How do we make a restricted transfer in accordance with the UK GDPR?
- Is the restricted transfer covered by an 'adequacy decision'?
- Is the restricted transfer covered by appropriate safeguards?
- Is the restricted transfer covered by an exception?

What are the restrictions on international transfers?

The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out.

Further Reading

 [Relevant provisions in the UK GDPR – see Article 44 and Recitals 101-102](#) 
External link

Are we making a transfer of personal data outside the UK?

1) Are we making a restricted transfer?

You are making a restricted transfer if:

- the UK GDPR applies to your processing of the personal data you are transferring.
- The scope of the UK data protection regime is set out in Articles 2 and 3 of the UK GDPR and section 207 DPA 2018 (where the DPA 2018, which incorporated the UK GDPR, applies). Please see the section of the guide [What is personal data](#).
- You are agreeing to send personal data, or make it accessible, to a receiver which is located in a country outside the UK; and
- the receiver is legally distinct from you as it is a separate company, organisation or individual. This includes transfers to another company within the same corporate group. However, if you are sending personal data to someone employed by you or by your company or organisation, this is not a restricted transfer. The transfer restrictions only apply if you are sending personal data outside your company or organisation.

Example

A UK company uses a centralised human resources service in the United States provided by its parent company. The UK company passes information about its employees to its parent company in connection with the HR service. This is a restricted transfer.

Example

A UK company sells holidays in Australia. It sends the personal data of customers who have bought the holidays to the hotels they have chosen in Australia in order to secure their bookings. This is a restricted transfer.

Transfer does not mean the same as transit. If personal data is just electronically routed through a non-UK country but the transfer is actually from one UK organisation to another, then it is not a restricted transfer.

Example

Personal data is transferred from a controller in the UK to another controller in the UK via a server in Australia. There is no intention that the personal data will be accessed or manipulated while it is in Australia. Therefore there is no restricted transfer.

You are making a restricted transfer if you collect information about individuals on paper, which is not ordered or structured in any way, and you send this to a service company located outside of the UK, to:

- put into digital form; or
- add to a highly structured manual filing system relating to individuals.

Example

A UK insurance broker sends a set of notes about individual customers to a company outside the UK. These notes are handwritten and are not stored on computer or in any particular order. The non-UK company adds the notes to a computer customer management system. This is a restricted transfer.

Putting personal data on to a website will often result in a restricted transfer. The restricted transfer

takes place when someone outside the UK accesses that personal data via the website.

If you load personal data onto a UK server which is then available through a website, and you plan or anticipate that the website may be accessed from outside the UK, you should treat this as a restricted transfer.

Further Reading

 Relevant provisions in the legislation - see UK GDPR Article 44 and Recital 101 

External link

 Data Protection and the EU

For organisations

Do we need to make a restricted transfer?

Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data.

If you make the data anonymous so that it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data. This means that the restrictions do not apply and you are free to transfer the anonymised data outside the UK.

Further Reading

 Relevant provisions in the legislation – see UK GDPR Article 44 and Recital 26 

External link

How do we make a restricted transfer in accordance with the UK GDPR?

You must work through the following questions, in order.

If by the last question, you are still unable to make the restricted transfer, then it will be in breach of the UK GDPR.

Is the restricted transfer covered by ‘adequacy regulations’?

You may make a restricted transfer if the receiver is located in a third country or territory or is an international organisation, covered by UK “adequacy regulations”.

UK “adequacy regulations” set out in law that the legal framework in that country, territory, sector or international organisation has been assessed as providing ‘adequate’ protection for individuals’ rights and freedoms for their personal data.

There are provisional arrangements so that UK “adequacy regulations” include the EEA and all countries, territories and international organisations covered by European Commission “adequacy decisions” valid as

at 31 December 2020. The UK intends to review these adequacy regulations over time.

1) What countries or territories are covered by adequacy regulations?

The UK has “adequacy regulations” in relation to the following countries and territories:

- The European Economic Area (EEA) countries.
 - These are the EU member states and the EFTA States.
 - The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
 - The EFTA states are Iceland, Norway and Liechtenstein.
- EU or EEA institutions, bodies, offices or agencies.
- Gibraltar.
- Countries, territories and sectors covered by the European Commission’s adequacy decisions (in force at 31 December 2020)
- These include a full finding of adequacy about the following countries and territories:
 - Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
- In addition, the partial findings of adequacy about:
 - Japan – only covers private sector organisations.
 - Canada - only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the [EU Commission's FAQs](#) on the adequacy finding on the Canadian PIPEDA.

2) What if there is no adequacy decision?

You should move on to the next section [Is the transfer covered by appropriate safeguards?](#)

Further Reading

 [Relevant provisions in the legislation – see UK GDPR Article 45 and Recitals 103-107 and 169](#) 
External link

Is the restricted transfer covered by appropriate safeguards?

If there are no UK ‘adequacy regulations’ about the country, territory or sector for your restricted transfer, you should then find out whether you can make the transfer subject to ‘appropriate safeguards’.

There is a list of appropriate safeguards in the UK GDPR. Each ensures that both you and the receiver of the restricted transfer are legally required to protect individuals’ rights and freedoms in respect of their personal data.

Have you undertaken a transfer impact assessment?

Before you may rely on an appropriate safeguard to make a restricted transfer, you must be satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.

You should do this by undertaking a risk assessment, which takes into account the protections contained in that appropriate safeguard and the legal framework of the destination country (including laws governing public authority access to the data).

If your assessment is that the appropriate safeguard does not provide the required level of protection, you may include additional measures.

This assessment is undoubtedly complex in many situations. The ICO intends to issue guidance on this topic in due course.

Further reading

The European Data Protection Board (EDPB) have published adopted [recommendations on measures that supplement transfer tools](#). The recommendations apply to the EU GDPR transfer regime, and are included here only as useful reference about additional measures. We will be producing our own guidance on this topic in due course.

Each appropriate safeguard is set out below:

1. A legally binding and enforceable instrument between public authorities or bodies

You can make a restricted transfer if it is covered by a legal instrument between public authorities or bodies containing 'appropriate safeguards'. The 'appropriate safeguards' must include enforceable rights and effective remedies for the individuals whose personal data is transferred.

This agreement or legal instrument could also be entered into with an international organisation.

Further Reading

 [Relevant provisions in the legislation – see UK GDPR Article 46 and Recitals 108-109 and 114](#) 
External link

2. Binding Corporate Rules (BCRs)

For information on Binding Corporate Rules, go to our [separate BCR page](#).

3. Standard contractual clauses (SCCs)

You can make a restricted transfer if you and the receiver have entered into a contract incorporating standard data protection clauses recognised or issued in accordance with the UK data protection regime. These are known as 'standard contractual clauses' ('SCCs' or 'model clauses').

The SCCs contain contractual obligations on you (the data exporter) and the receiver (the data importer), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those

rights against the data importer and the data exporter.

EU SCCs entered into prior to the end of the transitional period continue to be valid for restricted transfers under the UK regime.

The European Commission issued new EU SCCs on 04 June 2021. These are not valid for restricted transfers under UK GDPR (but see the next paragraph).

Following a consultation, the ICO has now issued new data protection clauses for restricted transfers, which will replace the old EU SCCs. [There is a new International Data Transfer Agreement \(IDTA\) and a new International Data Transfer Addendum to the new European Commission SCCs \(Addendum\)](#). These were laid before Parliament on 28 January 2022. Provided that there are no objections, these documents will be in force on 21 March 2022.

The ICO has also issued a document setting out transitional provisions regarding the current EU SCCs; this was also laid before Parliament on 28 January 2022.

You may continue to enter into new contracts on the basis of the old EU SCCs until 21 September 2022. All contracts on the basis of the old EU SCCs will continue to provide 'appropriate safeguards' for the purpose of UK GDPR, until 21 March 2024. From that date, if your restricted transfers continue, you must enter into a contract on the basis of the IDTA or the Addendum or find another way to make the restricted transfer under the UK GDPR.

When you are entering into a contract on the basis of the IDTA or the Addendum you must still carry out a risk assessment. This is to make sure that the actual protection provided by the IDTA or Addendum, given the actual circumstances of the restricted transfer, is sufficiently similar to the principles underpinning UK data protection laws.

Example

A family books a holiday in Australia with a UK travel company. The UK travel company sends details of the booking to the Australian hotel.

Each company is a separate controller, as it is processing the personal data for its own purposes and making its own decisions.

The contract between the UK travel company and the hotel should use controller to controller standard contractual clauses.

The UK travel company must also undertake a transfer impact assessment, and if necessary include additional measures to ensure that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.

If you are making a restricted transfer from a controller to a processor, you also need to comply with [the UK GDPR requirements about using processors](#).

Further Reading

The European Data Protection Board (EDPB) has adopted [recommendations on measures that supplement transfer tools](#). These recommendations apply to the EU GDPR transfer regime, and are included only as useful reference about additional measures. The ICO intends to issue its own guidance on this topic in due course.

Further Reading

 [Regulation \(EU\) 2016/679 of the European Parliament and of the Council](#)

External link

4. An approved code of conduct

You can make a restricted transfer if the receiver has signed up to a code of conduct, which has been approved by the ICO. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those appropriate safeguards.

The UK GDPR endorses the use of [approved codes of conduct](#) to demonstrate compliance with its requirements.

No approved codes of conduct are yet in use, but we are actively working with various sector bodies and associations. We will publish further information once codes of conduct are approved.

Further Reading

 [Relevant provisions in the legislation – see GDPR Article 46 and Recitals 108-109 and 114](#)

External link

In more detail - European Data Protection Board

The European Data Protection Board (EDPB) have published [guidance](#) on codes of conduct. This applies to the EU GDPR, and is included here as a useful reference. We will be producing our own guidance on this topic in due course.

5. Certification under an approved certification scheme

You can make a restricted transfer if the receiver has a certification, under a scheme approved by the ICO. The certification scheme must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those

appropriate safeguards.

The UK GDPR also endorses the use of [approved certification mechanisms](#) to demonstrate compliance with its requirements.

No approved certification schemes are yet in use as an appropriate safeguard for international transfers. The ICO will provide separate guidelines in relation to the use of certification schemes as a mechanism to facilitate international transfers in due course.

6. Contractual clauses authorised by the ICO

You can make a restricted transfer if you and the receiver have entered into a bespoke contract governing a specific restricted transfer which has been individually authorised by the ICO. This means that if you are making a restricted transfer from the UK, the ICO will have had to have approved the contract.

7. Administrative arrangements between public authorities or bodies

You can make a restricted transfer using:

- An administrative arrangement (usually a document, such as a memorandum of understanding) between public authorities or bodies.
- The administrative arrangement must set out 'appropriate safeguards' for the rights of the individuals whose personal data is to be transferred. The 'appropriate safeguards' must include effective and enforceable rights for the individuals whose personal data is transferred.
- The administrative arrangement must be individually authorised by the ICO.

Further Reading

 [Relevant provisions in the legislation – see GDPR Article 46 and Recitals 108-109 and 114](#) 
External link

What if the restricted transfer is not covered by appropriate safeguards?

If the restricted transfer is not covered by appropriate safeguards, then you need to consider the next question: [Is the restricted transfer covered by an exception?](#)

Is the restricted transfer covered by an exception?

If you are making a restricted transfer that is not covered by UK 'adequacy regulations', nor an appropriate safeguard, then you can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 of the UK GDPR.

You should only use these as true 'exceptions' from the general rule that you should not make a restricted transfer unless it is covered by UK 'adequacy regulations' or there are [appropriate safeguards](#) in place.

If it is covered by an exception, you may go ahead with the restricted transfer. Of course, you must still

comply with the rest of the UK GDPR.

Each exception is set out below:

Exception 1. Has the individual given his or her explicit consent to the restricted transfer?

Please see the [section on consent](#) as to what is required for a valid explicit consent under the UK GDPR.

As a valid consent must be both specific and informed, you must provide the individual with precise details about the restricted transfer. You cannot obtain a valid consent for restricted transfers in general.

You should tell the individual:

- the identity of the receiver, or the categories of receiver;
- the country or countries to which the data is to be transferred;
- why you need to make a restricted transfer;
- the type of data;
- the individual's right to withdraw consent; and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other [appropriate safeguards](#) in place. For example, you might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

Given the high threshold for a valid consent, and that the consent must be capable of being withdrawn, this may mean that using consent is not a feasible solution.

Exception 2. Do you have a contract with the individual? Is the restricted transfer necessary for you to perform that contract?

Are you about to enter into a contract with the individual? Is the restricted transfer necessary for you to take steps requested by the individual in order to enter into that contract?

This exception explicitly states that it can only be used for **occasional** restricted transfers. This means that the restricted transfer may happen more than once but not regularly. If you are regularly making restricted transfers, you should be putting in place an [appropriate safeguard](#).

The transfer must also be **necessary**, which means that you cannot perform the core purpose of the contract or the core purpose of the steps needed to enter into the contract, without making the restricted transfer. It does not cover a transfer for you to use a cloud based IT system.

Example

A UK travel company offering bespoke travel arrangements may rely on this exception to send personal data to a hotel in Peru, provided that it does not regularly arrange for its customers to stay at that hotel. If it did, it should consider using an appropriate safeguard, such as the [standard contractual clauses](#).

It is only necessary to send limited personal data for this purpose, such as the name of the guest, the

room required and the length of stay.

Example of necessary steps being taken at the individual's request in order to enter into a contract: Before the package is confirmed (and the contract entered into), the individual wishes to reserve a room in the Peruvian hotel. The UK travel company has to send the Peruvian hotel the name of the customer in order to hold the room.

Public authorities cannot rely on this exception when exercising their public powers.

Exception 3. Do you have (or are you entering into) a contract with an individual which benefits another individual whose data is being transferred? Is that transfer necessary for you to either enter into that contract or perform that contract?

As set out in Exception 2, you may only use this exception for occasional transfers, and the transfer must be necessary for you to perform the core purposes of the contract or to enter into that contract.

You may rely on both Exceptions 2 and 3: Exception 2 for the individual entering into the contract and Exception 3 for other people benefiting from that contract, often family members.

Exceptions 2 and 3 are not identical. You cannot rely on Exception 3 for any restricted transfers needed for steps taken prior to entering in to the contract.

Public authorities cannot rely on this exception when exercising their public powers.

Example

Following the Exception 2 example, Exception 3 may apply if the customer is buying the travel package for themselves and their family. Once the customer has bought the package with the UK travel company, it may be necessary to send the names of the family members to Peruvian hotel in order to book the rooms.

Exception 4: You need to make the restricted transfer for important reasons of public interest.

There must be a UK law which states or implies that this type of transfer is allowed for important reasons of public interest, which may be in the spirit of reciprocity for international co-operation. For example an international agreement or convention (which the UK has signed) that recognises certain objectives and provides for international co-operation (such as the [2005 International Convention for the Suppression of Acts of Nuclear Terrorism](#)).

This can be relied upon by both public and private entities.

If a request is made by a non-EEA authority, requesting a restrictive transfer under this exception, and there is an international agreement such as a mutual assistance treaty (MLAT), you should consider referring the request to the existing MLAT or agreement.

You should not rely on this exception for systematic transfers. Instead, you should consider one of the

[appropriate safeguards](#). You should only use it in specific situations, and each time you should satisfy yourself that the transfer is necessary for an important reason of public interest.

Exception 5: You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.

This exception explicitly states that you can only use it for **occasional** transfers. This means that the transfer may happen more than once but not regularly. If you are regularly transferring personal data, you should put in place an [appropriate safeguard](#).

The transfer must be necessary, so there must be a close connection between the need for the transfer and the relevant legal claim.

The claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures. This means that you can interpret what is a legal claim quite widely, to cover, for example:

- all judicial legal claims, in civil law (including contract law) and criminal law. The court procedure does not need to have been started, and it covers out-of-court procedures. It covers formal pre-trial discovery procedures.
- administrative or regulatory procedures, such as to defend an investigation (or potential investigation) in competition law or financial services regulation, or to seek approval for a merger.

You cannot rely on this exception if there is only the mere possibility that a legal claim or other formal proceedings may be brought in the future.

Public authorities can rely on this exception, in relation to the exercise of their powers.

Exception 6: You need to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.

This applies in a medical emergency where the transfer is needed in order to give the medical care required. The imminent risk of serious harm to the individual must outweigh any data protection concerns.

You cannot rely on this exception to carry out general medical research.

If the individual is physically and legally capable of giving consent, then you cannot rely on this exception.

For detail as to what is considered a 'vital interest' under the UK GDPR, please see [the section on vital interests as a condition of processing special category data](#).

For detail as to what is 'consent' under the UK GDPR please see the [section on consent](#).

Exception 7: You are making the restricted transfer from a public register.

The register must be created under UK law and must be open to either:

- the public in general; or
- any person who can demonstrate a legitimate interest.

For example, registers of companies, associations, land registers or public vehicle registers. The whole of the register cannot be transferred, nor whole categories of personal data.

The transfer must comply with any general laws which apply to disclosures from the public register. If the register has been established at law and access is only given to those with a legitimate interest, part of that assessment must take into account the data protection rights of the individuals whose personal data is to be transferred. This may include consideration of the risk to that personal data by transferring it to a country with less protection.

This does not cover registers run by private companies, such as credit reference databases.

Exception 8: you are making a one-off restricted transfer and it is in your compelling legitimate interests.

If you cannot rely on any of the other exceptions, there is one final exception to consider. This exception should not be relied on lightly and never routinely as it is only for truly exceptional circumstances.

For this exception to apply to your restricted transfer:

1. there must be no UK 'adequacy regulations' which apply.
2. you are unable to use any of the other appropriate safeguards. You must give serious consideration to this, even if it would involve significant investment from you.
3. none of the other exceptions apply. Again, you must give serious consideration to the other exceptions. It may be that you can obtain explicit consent with some effort or investment.
4. your transfer must not be repetitive – that is it may happen more than once but not regularly.
5. the personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise you must undertake in para (g) below.
6. The transfer must be necessary for your compelling legitimate interests. Please see the section of the guide on [legitimate interests as a lawful basis for processing](#), but bearing mind that this exception requires a higher standard, as it must be a compelling legitimate interest. An example is a transfer of personal data to protect a company's IT systems from serious immediate harm.
7. On balance your compelling legitimate interests outweigh the rights and freedoms of the individuals.
8. You have made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes, or sending pseudonymised or encrypted data. This must be recorded in full in your [documentation of your processing activities](#).
9. You have informed the ICO of the transfer. We will ask to see full details of all the steps you have taken as set out above.
10. You have informed the individual of the transfer and explained your compelling legitimate interest to them.

Further Reading

 [ICO analysis of the transfer of personal data from UK based firms to the US Securities and Exchange Commission ↗](#)

For organisations
PDF (266.95K)

Standard Contractual Clauses (SCCs) after the transition period ends

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

Once the transition period for leaving the EU ends, the UK will be able to produce its own SCCs for restricted transfers made from the UK. In the meantime, UK controllers can continue to use the existing EU SCCs (valid as at 31 December). See below for more detail.

The European Commission are consulting on [new draft SCCs](#), which we expect will be formally issued some time in 2021. This means they will not be valid SCCs for restricted transfers from the UK.

The recent Schrems II decision will continue to apply if you are making a restricted transfer from the UK using SCCs. This decision requires that you must make an assessment as to whether those SCCs provide protection which is 'essentially equivalent' to the protections in the UK data protection regime, and if necessary put in place additional measures.

This assessment is undoubtedly complex in many situations. The European Data Protection Board (EDPB) have published for consultation, [Recommendations on measures that supplement transfer tools](#). We expect the final version to be issued some time in 2021. The recommendations (when finalised) will apply to the EU GDPR transfer regime, and are included here only as useful reference about additional measures. The ICO intends to issue its own guidance on this topic in due course.

New Restricted Transfers from the UK

You can continue to use the current EU SCCs for restricted transfers from the UK.

You are able to make changes to those EU SCCs so they make sense in a UK context provided you do not change the legal meaning of the SCCs. For example, changing references from the old EU Data Protection to the UK GDPR, changing references to the EU or Member States, to the UK, and changing references to a supervisory authority to the ICO.

Otherwise you must not make any changes to the SCCs, unless it is to add protections or more clauses on business related issues. You can add parties (ie additional data importers or exporters) provided they are also bound by the SCCs.

We have created UK versions of the SCCs (with guidance), with suggested UK changes made for you.

Further Reading

-  [Standard contractual clauses for controllers to processors](#)
For organisations
Word (124.44K)

Standard contractual clauses for controllers to controllers ↗

For organisations
Word (113.07K)

Existing data transfers

After the transition period ends, you can continue to rely on existing SCCs which you have in place for restricted transfers from the UK. Although after the Schrems II decision, you should be reviewing whether they provide sufficient protection for data subjects and if necessary taking additional measures.

Future changes to SCCs

The ICO has consulted on UK SCCs and intends to publish them in 2022.

The ICO and the Secretary of State must keep the transitional arrangements for SCCs under review. It may be that at some point the EU SCCs will cease to be valid, for new and/or existing restricted transfers from the UK. The ICO will provide more information about this when this situation arises, giving you plenty of notice.

Further Reading

For more information about restricted transfers, read our guidance on [international transfers](#).

- [Art 46 UK GDPR ↗](#)
- [Schedule 21 DPA2018 ↗](#)

Existing EU SCCs:

- [2001 controller to controller](#)
- [2004 controller to controller](#)
- [2010 controller to processor](#)

International data transfer agreement and guidance

On 2 February 2022, the Secretary of State laid before Parliament the international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions. This final step followed the consultation the ICO ran in 2021. The documents were issued under Section 119A of the Data Protection Act 2018 and following Parliamentary approval came into force on 21 March 2022.

Exporters can use the IDTA or the Addendum as a transfer tool to comply with Article 46 of the UK GDPR when making restricted transfers.

The IDTA and Addendum replaced standard contractual clauses for international transfers. They take into account the binding judgement of the European Court of Justice, in the case commonly referred to as "Schrems II".

These documents are immediately of use to organisations transferring personal data outside of the UK:

- [International data transfer agreement \(PDF\)](#) ↗
- [International data transfer agreement \(Word document\)](#) ↗
- [International data transfer addendum to the European Commission's standard contractual clauses for international data transfers \(PDF\)](#) ↗
- [International data transfer addendum to the European Commission's standard contractual clauses for international data transfers \(Word document\)](#) ↗
- [Transitional provisions](#) ↗

The IDTA and Addendum form part of the wider UK package to assist international transfers. This includes independently supporting the Government's approach to adequacy assessments of third countries.

We consulted on our approach to international transfers under UK GDPR from 11 August 2021 to 11 October 2021. When finalising the documents we considered the detailed responses we received and will be publishing these soon.

In our Guide to UK GDPR we have added clarification as to what is a restricted transfer. We are developing additional tools to provide support and guidance to organisations. These will be published soon.

- Clause by clause guidance to the IDTA and Addendum.
- Guidance on how to use the IDTA.
- Guidance on transfer risk assessments.
- Further clarifications on our international transfers guidance.

Exemptions

At a glance

- The UK GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances.
- Whether or not you can rely on an exemption often depends on why you process personal data.
- You should not routinely rely on exemptions; you should consider them on a case-by-case basis.
- You should justify and document your reasons for relying on an exemption.
- If no exemption covers what you do with personal data, you need to comply with the UK GDPR as normal.

Checklists

Exemptions

- We consider whether we can rely on an exemption on a case-by-case basis.
- Where appropriate, we carefully consider the extent to which the relevant UK GDPR requirements would be likely to prevent, seriously impair, or prejudice the achievement of our processing purposes.
- We justify and document our reasons for relying on an exemption.
- When an exemption does not apply (or no longer applies) to our processing of personal data, we comply with the UK GDPR's requirements as normal.

In brief

- [What are exemptions?](#)
- [How do exemptions work?](#)
- [What exemptions are available?](#)

What are exemptions?

In some circumstances, the DPA 2018 provides an exemption from particular UK GDPR provisions. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain UK GDPR provisions.

This part of the Guide focuses on the exemptions in Schedules 2-4 of the DPA 2018. We give guidance on the exceptions built in to the UK GDPR in the parts of the Guide that relate to the relevant provisions.

The exemptions in the DPA 2018 can relieve you of some of your obligations for things such as:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal data breaches; and
- complying with the principles.

Some exemptions apply to only one of the above, but others can exempt you from several things.

Some things are not listed here as exemptions, although in practice they work a bit like an exemption. This is simply because they are not covered by the UK GDPR. Here are some examples:

- **Domestic purposes** – personal data processed in the course of a purely personal or household activity, with no connection to a professional or commercial activity, is outside the UK GDPR's scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the UK GDPR.
- **Law enforcement** – the processing of personal data by competent authorities for law enforcement purposes is outside the UK GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018. See our [Guide to Law Enforcement Processing](#) for further information.
- **Intelligence services processing** – personal data processed by the intelligence services (eg MI5) and their processors is outside the UK GDPR's scope. Instead, this type of processing is subject to the rules in Part 4 of the DPA 2018. See our [Guide to Intelligence Services Processing](#) for further information.

How do exemptions work?

Whether or not you can rely on an exemption generally depends on your purposes for processing personal data.

Some exemptions apply simply because you have a particular purpose. But others only apply to the extent that complying with the UK GDPR would:

- be likely to *prejudice* your purpose (e.g. have a damaging or detrimental effect on what you are doing); or
- *prevent* or *seriously impair* you from processing personal data in a way that is *required* or *necessary* for your purpose.

Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis.

If an exemption does apply, sometimes you will be obliged to rely on it (for instance, if complying with UK GDPR would break another law), but sometimes you can choose whether or not to rely on it.

In line with the accountability principle, you should justify and document your reasons for relying on an

exemption so you can demonstrate your compliance.

If you cannot identify an exemption that covers what you are doing with personal data, you must comply with the UK GDPR as normal.

What exemptions are available?

Crime, law and public protection

- Crime and taxation: general
- Crime and taxation: risk assessment
- Information required to be disclosed by law or in connection with legal proceedings
- Legal professional privilege
- Self incrimination
- Disclosure prohibited or restricted by an enactment
- Immigration
- Functions designed to protect the public
- Audit functions
- Bank of England functions

Regulation, parliament and the judiciary

- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Parliamentary privilege
- Judicial appointments, independence and proceedings
- Crown honours, dignities and appointments

Journalism, research and archiving

- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest

Health, social work, education and child abuse

- Health data – processed by a court
- Health data – an individual's expectations and wishes
- Health data – serious harm
- Health data – restriction of the right of access
- Social work data – processed by a court

- Social work data – an individual's expectations and wishes
- Social work data – serious harm
- Social work data – restriction of the right of access
- Education data – processed by a court
- Education data – serious harm
- Education data – restriction of the right of access
- Child abuse data

Finance, management and negotiations

- Corporate finance
- Management forecasts
- Negotiations

References and exams

- Confidential references
- Exam scripts and exam marks

Subject access requests – information about other people

- Protection of the rights of others

National security and defence

- National security and defence

Crime and taxation: general

There are two parts to this exemption. The first part can apply if you process personal data for the purposes of:

- the prevention and detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of a tax or duty or an imposition of a similar nature.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- notifying individuals of personal data breaches;
- the lawfulness, fairness and transparency principle, except the requirement for processing to be lawful;

- the purpose limitation principle; and
- all the other principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* your purposes of processing. If this is not so, you must comply with the UK GDPR as normal.

Example

A bank conducts an investigation into suspected financial fraud. The bank wants to pass its investigation file, including the personal data of several customers, to the National Crime Agency (NCA) for further investigation. The bank's investigation and proposed disclosure to the NCA are for the purposes of the prevention and detection of crime. The bank decides that, were it to inform the individuals in question about this processing of their personal data, this would be likely to prejudice the investigation because they might abscond or destroy evidence. So the bank relies on the crime and taxation exemption and, in this case, does not comply with the right to be informed.

The second part of this exemption applies when another controller obtains personal data processed for any of the purposes mentioned above for the purposes of discharging statutory functions. The controller that obtains the personal data is exempt from the UK GDPR provisions below to the same extent that the original controller was exempt:

- The right to be informed.
- The right of access.
- All the principles, but only so far as they relate to the right to be informed and the right of access.

Note that if you are a competent authority processing personal data for law enforcement purposes (e.g. the Police conducting a criminal investigation), your processing is subject to the rules of Part 3 of the DPA 2018. See our [Guide to Law Enforcement Processing](#) for information on how individual rights may be restricted when personal data is processed for law enforcement purposes by competent authorities.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 2](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\) and \(2\), 18\(1\), 19, 20\(1\) and \(2\), 21\(1\), and 34\(1\) and \(4\)](#) 
External link

Crime and taxation: risk assessment

This exemption can apply to personal data in a classification applied to an individual as part of a risk

assessment system.

The risk assessment system must be operated by a government department, local authority, or another authority administering housing benefit, for the purposes of:

- the assessment or collection of a tax or duty; or
- the prevention or detection of crime or the apprehension or prosecution of offenders, where the offence involves the unlawful use of public money or an unlawful claim for payment out of public money.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access;
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But the exemption only applies to the extent that complying with these provisions would *prevent* the risk assessment system from operating *effectively*. If this is not so, you must comply with these provisions as normal.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 3](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 
External link

Information required to be disclosed by law or in connection with legal proceedings

This exemption has three parts. The first part can apply if you are *required* by law to make personal data available to the public.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the lawfulness, fairness and transparency principle, except the requirement for processing to be lawful;
- the purpose limitation principle; and
- all the other principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would *prevent* you meeting your legal obligation to make personal data publicly available.

Example

The Registrar of Companies is legally obliged to maintain a public register of certain information about companies, including the names and (subject to certain restrictions) addresses of company directors. A director asks to exercise his right to erasure by having his name and address removed from the register. The request does not need to be complied with as it would prevent the Registrar meeting his legal obligation to make that information publicly available.

The second part of this exemption can apply if you are *required* by law, or court order, to disclose personal data to a third party. It exempts you from the same provisions as above, but only to the extent that complying with those provisions would *prevent* you disclosing the personal data.

Example

An employer receives a court order to hand over the personnel file of one of its employees to an insurance company for the assessment of a claim. Normally, the employer would not be able to disclose this information because doing so would be incompatible with the original purposes for collecting the data (contravening the purpose limitation principle). However, on this occasion the employer is exempt from the purpose limitation principle's requirements because it would prevent the employer disclosing personal data that it must do by court order.

The third part of this exemption can apply if it is *necessary* for you to disclose personal data for the purposes of, or in connection with:

- legal proceedings, including prospective legal proceedings;
- obtaining legal advice; or
- establishing, exercising or defending legal rights.

It exempts you from the same provisions as above, but only to the extent that complying with them would *prevent* you disclosing the personal data. If complying with these provisions would not prevent the disclosure, you cannot rely on the exemption.

Example

A primary school collects information about the parents of the children who attend the school. The school has informed the parents that they will only use their personal data for specified purposes related to the care, welfare and education of their children.

However, a dispute has arisen between a teacher and one of the parents of a 7 year old child. The

matter escalates, and the parent makes a number of allegations against the teacher. The school is concerned that the parent's behaviour is threatening and abusive, and decides to take legal action against them. The parent writes to the school and asks it not to share their information with any other organisation or individual.

The school relies on the exemption to the extent that complying with the request, and complying with the purpose limitation principle, would prevent it from disclosing the information to its solicitor.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 5](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Legal professional privilege

This exemption applies if you process personal data:

- to which a claim to legal professional privilege (or confidentiality of communications in Scotland) could be maintained in legal proceedings; or
- in respect of which a duty of confidentiality is owed by a professional legal adviser to their client.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 19](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 
External link

Self incrimination

This exemption can apply if complying with the UK GDPR provisions below would reveal evidence that you have committed an offence.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But the exemption only applies to the extent that complying with these provisions would expose you to proceedings for the offence.

This exemption does not apply to an offence under the DPA 2018 or an offence regarding false statements made otherwise than on oath.

But any information you do provide to an individual in response to a subject access request is not admissible against you in proceedings for an offence under the DPA 2018.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 20](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 

External link

Disclosure prohibited or restricted by an enactment

Five separate exemptions apply to personal data that is prohibited or restricted from disclosure by an enactment.

Each of them exempts you from the UK GDPR's provisions on:

- the right of access; and
- all the principles, but only so far as they relate to the right of access.

But the exemptions only apply to personal data restricted or prohibited from disclosure by certain specific provisions of enactments covering:

- human fertilisation and embryology;
- adoption;
- special educational needs;
- parental orders; and
- children's hearings.

If you think any of these exemptions might apply to your processing of personal data, see Schedule 4 of the DPA 2018 for full details of the enactments that are covered.

Further Reading

Relevant provisions in the Data Protection Act 2018 (the exemptions) - Schedule 4

External link

Relevant provisions in the UK GDPR (the exempt provisions) - Articles 5 and 15(1)-(3)

External link

Immigration

The exemption outlines specific rights in the UK GDPR which can be restricted if those rights would be likely to prejudice immigration matters.

The exemption can only be applied by the Secretary of State (including the Home Office and its agencies) when processing data for the purposes of maintaining effective immigration control, including investigatory/detection work (the immigration purposes).

The exemption is **not** available to other controllers who liaise with the Home Office on immigration matters.

The Secretary of State exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access;
- the right to erasure;
- the right to restrict processing;
- the right to object;
- all the principles, but only so far as they relate to the rights to be informed, of access, to erasure, to restrict processing and to object.

But the exemption only applies to the extent that applying these provisions would be likely to *prejudice* processing for the immigration purposes. If not, the exemption does not apply.

The Secretary of State is required to keep records of the use of the exemption and to inform individuals that the exemption has been applied unless it would be prejudicial to immigration purposes to inform them.

The exemption also requires that the Secretary of State has an immigration exemption policy document in place.

Further reading

The ICO has produced [detailed guidance on the immigration exemption](#).

[The Home Office has published its immigration exemption policy document here](#) .

Further Reading

Relevant provisions in the Data Protection Act 2018 (the exemption) - Schedule 2, Part 1, Paragraph 4

External link

 As amended by - The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022



External link

 Relevant provisions in the UK GDPR (the exempt provisions) – Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1) and 21(1) 

External link

Functions designed to protect the public

This exemption can apply if you process personal data for the purposes of discharging one of six functions designed to protect the public.

The first four functions must: be conferred on a person by enactment; be a function of the Crown, a Minister of the Crown or a government department; or be of a public nature and exercised in the public interest. These functions are:

1. to protect the public against financial loss due to the seriously improper conduct (or unfitness, or incompetence) of financial services providers, or in the management of bodies corporate, or due to the conduct of bankrupts;
2. to protect the public against seriously improper conduct (or unfitness, or incompetence);
3. to protect charities or community interest companies against misconduct or mismanagement in their administration, to protect the property of charities or community interest companies from loss or misapplication, or to recover the property of charities or community interest companies; or
4. to secure workers' health, safety and welfare or to protect others against health and safety risks in connection with (or arising from) someone at work.

The fifth function must be conferred by enactment on: the Parliamentary Commissioner for Administration; the Commissioner for Local Administration in England; the Health Service Commissioner for England; the Public Services Ombudsman for Wales; the Northern Ireland Public Services Ombudsman; the Prison Ombudsman for Northern Ireland; or the Scottish Public Services Ombudsman. This function is:

5. to protect the public from maladministration, or a failure in services provided by a public body, or from the failure to provide a service that it is a function of a public body to provide.

The sixth function must be conferred by enactment on the Competition and Markets Authority. This function is:

6. to protect members of the public from business conduct adversely affecting them, to regulate conduct (or agreements) preventing, restricting or distorting commercial competition, or to regulate undertakings abusing a dominant market position.

If you process personal data for any of the above functions, you are exempt from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and

- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If you can comply with these provisions and discharge your functions as normal, you must do so.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 7](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Audit functions

This exemption can apply if you process personal data for the purposes of discharging a function conferred by enactment on:

- the Comptroller and Auditor General;
- the Auditor General for Scotland;
- the Auditor General for Wales; or
- the Comptroller and Auditor General for Northern Ireland.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If it does not, you must comply with the UK GDPR as normal.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 8](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Bank of England functions

This exemption can apply if you process personal data for the purposes of discharging a function of the Bank of England:

- in its capacity as a monetary authority;
- that is a public function (within the meaning of Section 349 of the Financial Services and Markets Act 2000); or
- that is conferred on the Prudential Regulation Authority by enactment.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If this is not so, the exemption does not apply.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 1, Paragraph 9](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Regulatory functions relating to legal services, the health service and children's services

This exemption can apply if you process personal data for the purposes of discharging a function of:

- the Legal Services Board;
- considering a complaint under:
 - Part 6 of the Legal Services Act 2007,
 - Section 14 of the NHS Redress Act 2006,
 - Section 113(1) or (2), or Section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003,
 - Section 24D or 26 of the Children's Act 1989, or
 - Part 2A of the Public Services Ombudsman (Wales) Act 2005; or
- considering a complaint or representations under Chapter 1, Part 10 of the Social Services and Well-being (Wales) Act 2014.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If you can comply with these provisions and discharge your functions as normal, you cannot rely on the exemption.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 2, Paragraph 10](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Other regulatory functions

This exemption can apply if you process personal data for the purpose of discharging a regulatory function conferred under specific, listed legislation on any one of 14 bodies and persons. These are:

- the Information Commissioner;
- the Scottish Information Commissioner;
- the Pensions Ombudsman;
- the Board of the Pension Protection Fund;
- the Ombudsman for the Board of the Pension Protection Fund;
- the Pensions Regulator;
- the Financial Conduct Authority;
- the Financial Ombudsman;
- the investigator of complaints against the financial regulators;
- a consumer protection enforcer (other than the Competition and Markets Authority);
- the monitoring officer of a relevant authority;
- the monitoring officer of a relevant Welsh authority;
- the Public Services Ombudsman for Wales; or
- the Charity Commission.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;

- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your function. If this is not so, you must comply with these provisions as you normally would.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 2, Paragraphs 11-12](#)



External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) – Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), 21\(1\) and 34\(1\) and \(4\)](#)



Parliamentary privilege

This exemption can apply if it is *required* to avoid the privileges of either House of Parliament being infringed.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the communication of personal data breaches to individuals; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But if you can comply with these provisions without infringing parliamentary privilege, you must do so.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 2, Paragraph 13](#)



 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), 21\(1\), and 34\(1\) and \(4\)](#)



Judicial appointments, independence and proceedings

This exemption applies if you process personal data:

- for the purposes of assessing a person's suitability for judicial office or the office of Queen's Counsel;
- as an individual acting in a judicial capacity; or
- as a court or tribunal acting in its judicial capacity.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

Additionally, even if you do not process personal data for the reasons above, you are also exempt from the same provisions of the UK GDPR to the extent that complying with them would be likely to *prejudice* judicial independence or judicial proceedings.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 2, Paragraph 14](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 

External link

Crown honours, dignities and appointments

This exemption applies if you process personal data for the purposes of:

- conferring any honour or dignity by the Crown; or
- assessing a person's suitability for any of the following offices:
 - archbishops and diocesan and suffragan bishops in the Church of England,
 - deans of cathedrals of the Church of England,
 - deans and canons of the two Royal Peculiars,
 - the First and Second Church Estates Commissioners,
 - lord-lieutenants,
 - Masters of Trinity College and Churchill College, Cambridge,
 - the Provost of Eton,
 - the Poet Laureate, or
 - the Astronomer Royal.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 2, Paragraph 15](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 19, 20\(1\)-\(2\), and 21\(1\)](#) 

External link

Journalism, academia, art and literature

This exemption can apply if you process personal data for:

- journalistic purposes;
- academic purposes;
- artistic purposes; or
- literary purposes.

Together, these are known as the 'special purposes'.

The exemption relieves you from your obligations regarding the UK GDPR's provisions on:

- all the principles, except the security and accountability principles;
- the lawful bases;
- the conditions for consent;
- children's consent;
- the conditions for processing special categories of personal data and data about criminal convictions and offences;
- processing not requiring identification;
- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling;
- the communication of personal data breaches to individuals;
- consultation with the ICO for high risk processing;
- international transfers of personal data; and
- cooperation and consistency between supervisory authorities.

But the exemption only applies to the extent that:

- as controller for the processing of personal data, you reasonably believe that compliance with these provisions would be incompatible with the special purposes (this must be more than just an inconvenience);
- the processing is being carried out with a view to the publication of some journalistic, academic, artistic or literary material; and
- you reasonably believe that the publication of the material would be in the public interest, taking into account the special importance of the general public interest in freedom of expression, any specific public interest in the particular subject, and the potential to harm individuals.

When deciding whether it is reasonable to believe that publication would be in the public interest, you must (if relevant) have regard to:

- the BBC Editorial Guidelines;
- the Ofcom Broadcasting Code; and
- the Editors' Code of Practice.

We expect you to be able to explain why the exemption is required in each case, and how and by whom this was considered at the time. The ICO does not have to agree with your view – but we must be satisfied that you had a reasonable belief.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 5, Paragraph 26](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5\(1\)\(a\)-\(e\), 6, 7, 8\(1\)-\(2\), 9, 10, 11\(2\), 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\)\(a\)-\(b\) and \(d\), 19, 20\(1\)-\(2\), 21\(1\), 34\(1\) and \(4\), 36, 44, and 60-67](#) 

External link

Research and statistics

This exemption can apply if you process personal data for:

- scientific or historical research purposes; or
- statistical purposes.

It is unlikely to apply to the processing of personal data for commercial research purposes such as market research or customer satisfaction surveys, unless you can demonstrate that this research uses rigorous scientific methods and furthers a general public interest.

It exempts you from the UK GDPR's provisions on:

- the right of access;
- the right to rectification;
- the right to restrict processing; and
- the right to object.

The UK GDPR also provides exceptions from its provisions on the right to be informed (for indirectly collected data) and the right to erasure.

But the exemption and the exceptions only apply:

- to the extent that complying with the provisions above would *prevent or seriously impair* the achievement of the purposes for processing;
- if the processing is subject to appropriate safeguards for individuals' rights and freedoms (see Article 89(1) of the UK GDPR – among other things, you must implement data minimisation measures);
- if the processing is not likely to cause substantial damage or substantial distress to an individual;
- if the processing is not used for measures or decisions about particular individuals, except for approved medical research; and
- as regards the right of access, the research results are not made available in a way that identifies individuals.

Additionally, the UK GDPR contains specific provisions that adapt the application of the [purpose limitation](#) and [storage limitation](#) principles when you process personal data for scientific or historical research purposes, or statistical purposes. See the Guide pages on these principles for more detail.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 6, Paragraph 27](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5\(1\)\(b\) and \(e\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 18\(1\) and 21\(1\)](#) 
External link

Archiving in the public interest

This exemption can apply if you process personal data for archiving purposes in the public interest.

It exempts you from the UK GDPR's provisions on:

- the right of access;
- the right to rectification;
- the right to restrict processing;
- the obligation to notify others regarding rectification, erasure or restriction;
- the right to data portability; and
- the right to object.

The UK GDPR also provides exceptions from its provisions on the right to be informed (for indirectly collected data) and the right to erasure.

But the exemption and the exceptions only apply:

- to the extent that complying with the provisions above would prevent or seriously impair the

achievement of the purposes for processing;

- if the processing is subject to appropriate safeguards for individuals' rights and freedoms (see Article 89(1) of the UK GDPR – among other things, you must implement data minimisation measures);
- if the processing is not likely to cause substantial damage or substantial distress to an individual; and
- if the processing is not used for measures or decisions about particular individuals, except for approved medical research.

Additionally, the UK GDPR contains specific provisions that adapt the application of the [purpose limitation](#) and [storage limitation](#) principles when you process personal data for archiving purposes in the public interest. See the Guide pages on these principles for more detail.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 6, Paragraph 28](#) 
External link

 [Relevant provisions in the GDPR \(the exempt provisions\) - Articles 5\(1\)\(b\) and \(e\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 18\(1\), 19, 20\(1\) and 21\(1\)](#) 
External link

 [Relevant provisions in the GDPR \(the appropriate safeguards\) - Article 89\(1\) and Recital 156](#) 
External link

 [Relevant provisions in the Data Protection Act 2018 \(safeguards\) - Section 19](#) 
External link

Further reading – The National Archives

The National Archives is the official archive and publisher for the UK Government and for England and Wales. It has published a detailed [guide to archiving personal data](#) .

Further reading - ICO guidance

The ICO has produced [guidance on the research provisions](#).

Health data – processed by a court

This exemption can apply to health data (personal data concerning health) that is processed by a court.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;

- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies if the health data is:

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the data to be withheld from the individual it relates to.

If you think this exemption might apply to your processing of personal data, see paragraph 3(2) of Schedule 3, Part 2 of the DPA 2018 for full details of the statutory rules.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 2, Paragraph 3](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Health data – an individual's expectations and wishes

This exemption can apply if you receive a request (in exercise of a power conferred by an enactment or rule of law) for health data from:

- someone with parental responsibility for an individual aged under 18 (or 16 in Scotland); or
- someone appointed by the court to manage the affairs of an individual who is incapable of managing their own affairs.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with the request would disclose information that:

- the individual provided in the expectation that it would not be disclosed to the requestor, unless the individual has since expressly indicated that they no longer have that expectation;
- was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or

- the individual has expressly indicated should not be disclosed in this way.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 2, Paragraph 4](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 20\(1\)-\(2\), and 21\(1\)](#) 
External link

Health data – serious harm

This exemption can apply if you receive a subject access request for health data.

It exempts you from the UK GDPR's provisions on the right of access regarding your processing of health data.

But the exemption only applies to the extent that compliance with the right of access would be likely to cause *serious harm* to the *physical or mental health* of any individual. This is known as the 'serious harm test' for health data.

You can only rely on this exemption if:

- you are a health professional; or
- within the last six months you have obtained an opinion from an appropriate health professional that the serious harm test for health data is met. Even if you have done this, you still cannot rely on the exemption if it would be reasonable in all the circumstances to re-consult the appropriate health professional.

If you think this exemption might apply to a subject access request you have received, see paragraph 2(1) of Schedule 3, Part 2 of the DPA 2018 for full details of who is considered an appropriate health professional.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 2, Paragraph 5](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Health data – restriction of the right of access

This is a restriction rather than an exemption. It applies if you receive a subject access request for health data.

It restricts you from disclosing health data in response to a subject access request, unless:

- you are a health professional; or
- within the last six months you have obtained an opinion from an appropriate health professional that the serious harm test for health data is *not* met. Even if you have done this, you must re-consult the appropriate health professional if it would be reasonable in all the circumstances.

This restriction does not apply if you are satisfied that the health data has already been seen by, or is known by, the individual it is about.

If you think this restriction could apply to a subject access request you have received, see paragraph 2(1) of Schedule 3, Part 2 of the DPA 2018 for full details of who is considered an appropriate health professional.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 2, Paragraph 6](#) 
External link

 [Relevant provisions in the UK GDPR \(the restricted provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Social work data – processed by a court

This exemption can apply to social work data (personal data that isn't health or education data) processed by a court. If you are unsure whether the data you process is social work data, see paragraphs 7(1) and 8 of Schedule 3, Part 3 of the DPA 2018 for full details of what this is.

The exemption relieves you from your obligations regarding the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies if the social work data is:

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the social work data to be withheld from the individual it relates to.

If you think this exemption might apply to your processing of personal data, see paragraph 9(2) of Schedule 3, Part 3 of the DPA 2018 for full details of the statutory rules.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 3, Paragraph 9](#) 

External link

↗ Relevant provisions in the UK GDPR (the exempt provisions) - Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), and 21(1) ↗

External link

Social work data – an individual’s expectations and wishes

This exemption can apply if you receive a request (in exercise of a power conferred by an enactment or rule of law) for social work data concerning an individual from:

- someone with parental responsibility for an individual aged under 18 (or 16 in Scotland); or
- someone appointed by court to manage the affairs of an individual who is incapable of managing their own affairs.

It exempts you from the UK GDPR’s provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies to the extent that complying with the request would disclose information that:

- the individual provided in the expectation that it would not be disclosed to the requestor, unless the individual has since expressly indicated that they no longer have that expectation;
- was obtained as part of an examination or investigation to which the individual consented in the expectation that the information would not be disclosed in this way, unless the individual has since expressly indicated that they no longer have that expectation; or
- the individual has expressly indicated should not be disclosed in this way.

Further Reading

↗ Relevant provisions in the Data Protection Act 2018 (the exemption) - Schedule 3, Part 3, Paragraph 10 ↗

External link

↗ Relevant provisions in the UK GDPR (the exempt provisions) - Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), 20(1)-(2), and 21(1) ↗

External link

Social work data – serious harm

This exemption can apply if you receive a subject access request for social work data.

It exempts you from the UK GDPR’s provisions on the right of access regarding your processing of social

work data.

But the exemption only applies to the extent that complying with the right of access would be likely to prejudice carrying out social work because it would be likely to cause *serious harm* to the *physical or mental health* of any individual. This is known as the 'serious harm test' for social work data.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 3, Paragraph 11](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Social work data – restriction of the right of access

This is a restriction rather than an exemption. It applies if you process social work data as a local authority in Scotland (as defined by the Social Work (Scotland) Act 1968), and you receive a subject access request for that data.

It restricts you from disclosing social work data in response to a subject access request if:

- the data came from the Principal Reporter (as defined by the Children's Hearings (Scotland) Act 2011) in the course of his statutory duties; and
- the individual whom the data is about is not entitled to receive it from the Principal Reporter.

If there is a question as to whether you need to comply with a subject access request in this situation, you must inform the Principal Reporter within 14 days of the question arising.

You must not disclose the social work data in response to the subject access request unless the Principal Reporter has told you they think the serious harm test for social work data is not met.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 3, Paragraph 12](#) 
External link

 [Relevant provisions in the UK GDPR \(the restricted provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Education data – processed by a court

This exemption can apply to education data (personal data in an educational record) processed by a court. If you are unsure whether the data you process is 'education data', see paragraphs 13-17 of Schedule 3, Part 4 of the DPA 2018 for full details of what this is.

The exemption relieves you from your obligations regarding the UK GDPR's provisions on:

- the right to be informed;
- all the other individual rights, except rights related to automated individual decision-making including profiling; and
- all the principles, but only so far as they relate to the right to be informed and the other individual rights.

But the exemption only applies if the education data is:

- supplied in a report or evidence given to the court in the course of proceedings; and
- those proceedings are subject to certain specific statutory rules that allow the education data to be withheld from the individual it relates to.

If you think this exemption might apply to your processing of personal data, see paragraph 18(2) of Schedule 3, Part 4 of the DPA 2018 for full details of the statutory rules.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 4, Paragraph 18](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), 15\(1\)-\(3\), 16, 17\(1\)-\(2\), 18\(1\), 20\(1\)-\(2\), and 21\(1\)](#) 

External link

Education data – serious harm

This exemption can apply if you receive a subject access request for education data.

It exempts you from the UK GDPR's provisions on the right of access regarding your processing of education data.

But the exemption only applies to the extent that complying with the right of access would be likely to cause *serious harm* to the *physical* or *mental health* of any individual. This is known as the 'serious harm test' for education data.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 4, Paragraph 19](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Article 15\(1\)-\(3\)](#) 

External link

Education data – restriction of the right of access

This is a restriction rather than an exemption. It applies if you process education data as an education

authority in Scotland (as defined by the Education (Scotland) Act 1980), and you receive a subject access request for that data.

It restricts you from disclosing education data in response to a subject access request if:

- you believe that the data came from the Principal Reporter (as defined by the Children's Hearings (Scotland) Act 2011) in the course of his statutory duties; and
- the individual whom the data is about is not entitled to receive it from the Principal Reporter.

If there is a question as to whether you need to comply with a subject access request in this situation, you must inform the Principal Reporter within 14 days of the question arising.

You must not disclose the education data in response to the subject access request unless the Principal Reporter has told you they think the serious harm test for education data is not met.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 4, Paragraph 20](#) 
External link

 [Relevant provisions in the UK GDPR \(the restricted provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Child abuse data

This exemption can apply if you receive a request (in exercise of a power conferred by an enactment or rule of law) for child abuse data. If you are unsure whether the data you process is 'child abuse data', see paragraph 21(3) of Schedule 3, Part 5 of the DPA 2018 for a definition.

The exemption applies if the request is from:

- someone with parental responsibility for an individual aged under 18; or
- someone appointed by court to manage the affairs of an individual who is incapable of managing their own affairs.

It exempts you from the UK GDPR's provisions on the right of access.

But the exemption only applies to the extent that complying with the request would not be in the best interests of the individual who the child abuse data is about.

This exemption can only apply in England, Wales and Northern Ireland. It cannot apply in Scotland.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 3, Part 5](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Article 15\(1\)-\(3\)](#) 
External link

Corporate finance

This exemption can apply if you process personal data in connection with a corporate finance service (e.g. if you underwrite financial instruments or give corporate finance advice to undertakings) that you are permitted to provide (as set out in the Financial Services and Markets Act 2000).

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But the exemption only applies to the extent that complying with the provisions above would:

- be likely to affect the price of an instrument; or
- have a prejudicial effect on the orderly functioning of financial markets (or the efficient allocation of capital within the economy), and you reasonably believe that complying with the provisions above could affect someone's decision whether to:
 - deal in, subscribe for or issue a financial instrument, or
 - act in a way likely to have an effect on a business activity (e.g. an effect on an undertaking's capital structure, the legal or beneficial ownership of a business or asset or a person's industrial strategy)

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 21](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 
External link

Management forecasts

This exemption can apply if you process personal data for the purposes of management forecasting or management planning in relation to a business or other activity.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But the exemption only applies to the extent that compliance with the above provisions would be likely to *prejudice* the conduct of the business or activity.

Example

The senior management of an organisation is planning a re-organisation. This is likely to involve making certain employees redundant, and this possibility is included in management plans. Before the plans are revealed to the workforce, an employee makes a subject access request. In responding to that request, the organisation does not have to reveal its plans to make him redundant if doing so would be likely to prejudice the conduct of the business (perhaps by causing staff unrest before the management's plans are announced).

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 22](#) 
External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 
External link

Negotiations

This exemption can apply to personal data in records of your intentions relating to any negotiations with an individual.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But it only applies to the extent that complying with the above provisions would be likely to *prejudice* negotiations with that individual.

Example

An individual makes a claim to his insurance company. The claim is for compensation for personal injuries he sustained in an accident. The insurance company disputes the seriousness of the injuries and the amount of compensation it should pay. An internal paper sets out the company's position on these matters including the maximum sum it would be willing to pay to avoid the claim going to court. If the individual makes a subject access request to the insurance company, it would not have to send him the internal paper – because doing so would be likely to prejudice the negotiations to settle the claim.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 23](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 

External link

Confidential references

This exemption applies if you give or receive a confidential reference for the purposes of prospective or actual:

- education, training or employment of an individual;
- placement of an individual as a volunteer;
- appointment of an individual to office; or
- provision by an individual of any service.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

Example

Company A provides an employment reference in confidence for one of its employees to company B. If the employee makes a subject access request to company A or company B, the reference will be exempt from disclosure. This is because the exemption applies to the reference regardless of whether it

is in the hands of the company that gives it or receives it.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 24](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) - Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 

External link

Exam scripts and exam marks

This exemption can apply to personal data in exam scripts.

It exempts you from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

But it only applies to the information recorded by candidates. This means candidates do not have the right to copies of their answers to the exam questions.

However, the information recorded by the person marking the exam is not exempt from the above provisions. If an individual makes a subject access request for this information before the results are announced, special rules apply to how long you have to comply with the request. You must provide the information:

- within five months of receiving the request; or
- within 40 days of announcing the exam results, if this is earlier.

Further Reading

 [Relevant provisions in the Data Protection Act 2018 \(the exemption\) - Schedule 2, Part 4, Paragraph 25](#) 

External link

 [Relevant provisions in the UK GDPR \(the exempt provisions\) – Articles 5, 13\(1\)-\(3\), 14\(1\)-\(4\), and 15\(1\)-\(3\)](#) 

External link

The above information applies to pupil information assessments being undertaken instead of exams during the coronavirus outbreak.

Further Reading

Protection of the rights of others

Paragraphs 16 and 17 of Schedule 2, Part 3 of the DPA 2018 provide an exemption that can apply if you receive a subject access request for information containing the personal data of more than one individual.

Further reading

For guidance on what to do if you receive a request for information that includes the personal data of other people, see our [Guide page on the right of access](#).

National security and defence

If you are processing personal data to safeguard national security or for defence purposes, there is an exemption provided for at section 26 of the DPA 2018. You may be able to apply this exemption if you process data under the UK GDPR.

National security is not specifically defined but it can cover processing for:

- 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.

If the exemption applies, it can exempt you from:

- any of the data protection principles (except lawfulness requirements);
- any of the rights of individuals;
- personal data breach reporting;
- international transfers requirements; and
- some of the Commissioner's duties and enforcement powers.

You must always ensure that your processing is lawful, and that you have a lawful basis under Article 6. There is no exemption from the requirement to process lawfully.

You must always comply with your general accountability and governance obligations.

If you are processing special category data for national security purposes there is no exemption from Article 9, but special rules apply. Section 28 of the DPA permits the processing of special category data for safeguarding national security, provided you ensure there are appropriate safeguards for the rights and freedoms of data subjects.

This is not a blanket exemption. You must be able to show that the exemption from specified data protection standards is required for the purposes of safeguarding national security. When deciding whether

Immigration exemption

About this guidance

This guidance discusses the immigration exemption in detail. Read it if you have detailed questions not answered in the guide, or if you need a deeper understanding to help you apply this exemption in practice. It is aimed at DPOs and those with specific data protection responsibilities in larger organisations.

If you haven't yet read the '[in brief' page on the immigration exemption](#) in the Guide to Data Protection, you should read that first. It introduces this topic and sets out the key points you need to know, along with practical checklists to help you comply.

In detail

- [What is the immigration exemption?](#)
- [When should this exemption be used?](#)
- [What is an immigration exemption policy document?](#)
- [What is the prejudice test?](#)
- [What rights does the immigration exemption apply to?](#)
- [How does the exemption affect the individual's right to be informed?](#)
- [How does the exemption affect the individual's right of access?](#)
- [Do we need to inform individuals that the immigration exemption has been applied?](#)
- [What happens if an immigration investigation becomes a criminal investigation?](#)

What is the immigration exemption?

The exemption outlines specific rights in the UK GDPR which can be restricted if those rights would be likely to prejudice immigration matters.

The exemption can only be applied by the Secretary of State (including the Home Office and its agencies) who processes data for the purposes of:

- the maintenance of effective immigration control; or
- the investigation or detection of activities that would undermine the maintenance of effective immigration control.

It is **not** available to other controllers, such as employers, universities and the police, who liaise with the Home Office on immigration matters.

It also requires that the Secretary of State has an immigration exemption policy document in place.

The exemption is set out in Schedule 2 Part 1 Paragraph 4 of the Data Protection Act 2018, and has been amended by The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022. The amendments came into force on 31 January 2022 in response to a court judgment. The amendments

introduce further safeguards to the exemption including limiting its use to the Secretary of State, requiring an immigration exemption policy document, and a requirement to keep records and inform individuals that the exemption has been used.

In the UK, the right to appeal is an integral part of immigration control. Individuals have the right to have their immigration applications reviewed and to submit an appeal against an asylum decision or a deportation order.

You should ensure that you are not undermining this review and appeals system process by using this exemption. For example, by refusing an individual access to their personal data.

You should only restrict the exercising of a data subject's rights if the exemption applies and there is a valid reason to apply it.

Your application of the exemption must be proportionate to the circumstances and you must carefully consider and document each instance. You should not apply the immigration exemption as a blanket restriction on the data protection rights of individuals, such as migrants or people who have overstayed their permission to remain. You should only apply it, if required, when the exercise of those rights is likely to cause prejudice to effective immigration control. You must apply the exemption on a case by case basis. You must have regard to your immigration exemption policy document when deciding if the exemption applies.

Example

An individual seeking asylum in the UK has had their application refused. They make a request to the Home Office for all their personal data so that they can appeal against this decision.

The Home Office is not investigating the individual and can provide the personal data it holds without prejudice to its immigration control function. It does not hold any confidential intelligence (a factor listed for consideration in its immigration exemption policy document) which the individual is unaware of and it has no reason to withhold any of the requested personal data. It must not use the exemption to frustrate a lawful appeal.

In these circumstances the exemption does not apply and should not be used. The Home Office should therefore disclose the information it holds.

There are various immigration offences (eg overstaying leave to remain) and these are usually dealt with by the administrative removal of the offender rather than through the criminal justice process. Therefore the '[crime and taxation' exemption](#)' does not usually apply in circumstances where immigration control is concerned. However the two exemptions involve similar considerations. Instead of considering prejudice to the apprehension or prosecution of offenders, the immigration exemption requires you to consider prejudice to the administrative functions concerning effective immigration control.

There is no assumption of criminal proceedings with the immigration exemption, although the section below considers [what happens if an immigration investigation does become a criminal investigation](#).

As noted above, this exemption is only available to the Secretary of State, which includes the Home Office and its agencies, who are engaged in immigration control.

Further Reading

 [Relevant provisions in the DPA 2018 \(the exemption\) - See DPA 2018 Schedule 2, Part 1, Paragraph 4](#) 

External link

 [The Data Protection Act 2018 \(Amendment of Schedule 2 Exemptions\) Regulations 2022](#) 

External link

When should this exemption be used?

The immigration exemption applies to specific rights in the UK GDPR which can be restricted **to the extent that** giving effect to those rights **would be likely to prejudice**:

- the maintenance of effective immigration control; or
- the investigation or detection of activities that would undermine the maintenance of effective immigration control.

The phrase 'to the extent that' means that you should not apply the immigration exemption as a blanket exemption to restrict all of those rights for all the data you hold. Instead, you need to consider the application of the exemption on a case by case basis, taking into account your immigration exemption policy document.

The scope of the exemption is limited to those rights which, if exercised for the data held, would prejudice the identified immigration purposes. The exemption therefore only applies when the exercise of the specific right results in the processing of personal data which would be likely to prejudice the identified function.

Therefore the default position of the controller should be to comply with the requirements of the UK GDPR and the DPA 2018 as far as possible. It highlights the importance of identifying the specific reason for applying the exemption in each case.

Many of the rights set out in the UK GDPR contain built-in restrictions or exceptions. The expectation is that you should rely on these more generic built-in restrictions in preference to the immigration exemption, if they can achieve the same outcome. This is because the immigration exemption (along with the other exemptions set out in Schedules 2-4 of the DPA 2018) is an exemption for a specific purpose, and can only be used if applying the usual provisions of the UK GDPR would cause a specific problem.

You should therefore first consider the restrictions to an individual's rights as laid out in other relevant UK GDPR articles. For example, you should consider whether an objection to processing is valid under Article 21, or whether you should allow or refuse an individual exercising their right under Article 17.

You should only use the immigration exemption in circumstances where there are no viable alternatives.

For further information on the individual's data protection rights see our UK GDPR guidance [Individual rights](#).

Example

An individual with Leave to Remain in the UK applies to the Home Office to have their personal data erased. The individual is under investigation for an immigration offence.

The personal data held is still necessary for the purpose it was originally collected for, and the Home Office can rely on Article 17(3)(b) to refuse the request. This is because the right to erasure does not apply if personal data needs to be retained for:

- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject; or
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In this case, the restriction of the individual's rights is accomplished without relying on the immigration exemption.

Further Reading

 [Relevant provisions in the UK GDPR - See UK GDPR Articles 17\(3\)\(b\)](#) 

External link

What is an immigration exemption policy document?

In order to be able to apply the exemption, the Secretary of State must have an immigration exemption policy document in place.

The immigration exemption policy document must explain the policies and processes the Secretary of State (including the Home Office and its agencies) will use to decide how compliance with a provision under the UK GDPR would be likely to prejudice the carrying out of effective immigration control. For example, it should describe the factors the organisation will consider when making the decision in each case.

The document must also explain the policies in place to make sure that the use of the immigration exemption does not allow personal data to be abused, accessed, or transferred in a manner that does not comply with the UK GDPR.

When considering whether the immigration exemption applies, the Secretary of State must have regard to the immigration exemption policy document.

The Secretary of State must also:

- review the immigration exemption policy document and (if necessary) update it from time to time; and
- publish it.

Further reading

The Home Office has published its immigration exemption policy document here [↗](#).

What is the prejudice test?

The DPA 2018 does not explain what is meant by 'would be likely to prejudice'. However, the ICO's view is there must be a real and substantial chance of prejudice, rather than just a hypothetical or remote possibility that complying with the provision would noticeably damage the discharge of the function concerned.

There should be a causal link between compliance and the prejudice claimed, and you must be able to show how the exercising of a specific right would be likely to lead to the prejudice. In reaching a decision on this, you should take into account the immigration exemption policy document. You must make this reasoning available to the ICO if required.

The prejudice test has a high threshold and you should not apply the exemption in a blanket fashion. It must be both necessary and proportionate to apply the exemption and you must only apply it to specific rights where the likelihood of prejudice is present, rather than applying this across the board to all the rights.

You must consider whether the application of the exemption is a proportionate response. You may consider that there is a pressing social need to apply the immigration exemption, but you must also take into account whether this outweighs your obligation to individuals under the UK GDPR. They have rights over their personal data which you must consider in all circumstances, in particular, the right of access.

It is therefore important in every case that you consider whether the data protection rights of the individual override the identified risk of prejudice. Your application of the exemption must be proportionate to the circumstances and you must carefully consider and document each instance.

It is also important to note that prejudice changes over time. While personal data may be withheld during an ongoing investigation, disclosure of this information is unlikely to present the same risk afterwards.

Therefore, you should keep the immigration exemption under review. You should always consider an individual's current circumstances. For example, you should not assume that if you have once refused to provide a data subject with all their personal data under this exemption, then your response will always remain the same. Should they submit a new subject access request to you, you should assess whether circumstances have changed and whether providing the data would now prejudice the maintenance of effective immigration control. If not, you may be able to respond more fully to this new request.

Example

An individual is suspected of overstaying their student visa in the UK. While an investigation is carried out, they make a request for all personal data held about them.

The Home Office may withhold information which, if disclosed, will prejudice the investigation. This might include information which identifies any proposed actions against the individual.

However the Home Office should not apply a blanket exemption. It could disclose any personal data relating to the individual's previous visa application and any other information it holds, unless it can show that the disclosure will be likely to impact on the ongoing investigation or any expected actions arising from it.

The individual successfully extends their visa due to extenuating circumstances and is allowed to remain in the UK for another two years. They make another request for their personal data.

The Home Office will have to carefully consider this, taking into account the guidance set out in the immigration exemption policy document. As there are no active proceedings against the individual, the exemption will only continue to be available if there is any remaining prejudice to immigration controls, and the Home Office should not use it simply because it applied previously.

Although the immigration exemption may no longer apply in this context, other exemptions under Schedule 2 of the DPA 2018 may be relevant.

More information is available in our detailed freedom of information guidance [The prejudice test](#).

What rights does the immigration exemption apply to?

The exemption applies to the following rights:

- right to be informed;
- right of access;
- right to erasure;
- right to restrict processing; and
- right to object.

The exemption does not restrict other data subject rights. More information is available in our UK GDPR guidance on [Individual rights](#).

Example

An individual being investigated for an immigration offence contacts the Home Office to request that their date of birth is rectified, as this is inaccurately reflected in their records.

The right to rectification is not a right which is restricted under this exemption. The Home Office must therefore update their records and respond to the individual within the time frame permitted.

Further Reading

 Relevant provisions in the UK GDPR (the exempt provisions) - See UK GDPR Articles 5, 13(1)-(3), 14(1)-(4), 15(1)-(3), 17(1)-(2), 18(1) and 21(1) 
External link

How does the exemption affect the individual's right to be informed?

The right to be informed means that the data subject has the right to be given certain privacy information about the processing of their data. This includes for example, the purposes of the processing and the identity and contact details of the controller. This applies whether you obtain personal data from the individual or from someone else.

The provision of this privacy information also meets the transparency requirement of Article 5(a).

However, if you are investigating an individual, you may not wish to tell them that you are processing their personal data for the purposes of immigration control. This would alert them to your investigation, and would be likely to prejudice the purpose of the processing.

In these circumstances, you may apply the immigration exemption and restrict the individual's right to be informed. You do not have to provide privacy information if this is likely to prejudice the identified immigration purposes.

As discussed above, the immigration exemption also provides an exemption from the data protection principles so far as their provisions correspond to the listed data subject rights. Therefore in these circumstances, it provides an exemption from the transparency requirement of Article 5(a) to the extent that this corresponds with the right to be informed.

However, although you may therefore be exempt from providing privacy information to the individual you are investigating, you still have to comply with the other requirements of Article 5(a) and identify a lawful basis for processing. This lawfulness part of Article 5(a) does not affect (or correspond to) any of the rights listed above and so you are not exempt from this particular obligation.

More information is available in our UK GDPR guidance [Right to be informed](#).

Further Reading

 Relevant provisions in the UK GDPR - See UK GDPR Articles 5, 13 and 14 and Recitals 39, 60 and 61 
External link

How does the exemption affect the individual's right of access?

An individual may make a subject access request to you, in order to obtain a copy of the data you hold about them. You must consider the circumstances of each case and may apply the exemption only if you consider that to comply with the right of access would be likely to prejudice effective immigration control.

You may not wish to provide a copy of all the personal data you hold, if this would prejudice a current investigation into that individual's immigration status, or would otherwise prejudice the maintenance of effective immigration controls. However, you may be able to provide some personal data in response to the

request, if this does not prejudice your investigation.

More information is available in our UK GDPR guidance [Right of access](#).

Example

An individual who has been refused entry to the UK at an airport e-Passport gate makes a Subject Access Request to the Home Office, asking for information about why their entry was refused.

Providing the individual with this information would involve disclosing details about the technical operation of the e-Passport gates, which if made public, could have a detrimental effect on border control, potentially enabling attempts to undermine the system.

In this case, the Home Office may legitimately rely on the immigration exemption as a reason to refuse to disclose the requested information.

Do we need to inform individuals that the immigration exemption has been applied?

You should keep a record of the decision to apply the immigration exemption, and your reasoning, each time it is applied. Individuals should be informed that the immigration exemption has been applied unless it would be prejudicial to effective immigration control to do so. See 'What is the prejudice test?' for guidance on how to assess whether an individual being informed that the immigration exemption has been used would be prejudicial to carrying out immigration control.

Example

An individual seeking asylum in the UK has had their application refused. They make a request to the Home Office for all their personal data so that they can appeal against this decision.

The Home Office is investigating them for the use of identification which does not belong to them and it would prejudice the investigation to provide them with the personal data relating to this investigation.

The Home Office therefore may apply this exemption in order to restrict the individual's right of access. However it should provide as much data as it can and inform the individual where the immigration exemption has been applied, if this does not prejudice the investigation.

What happens if an immigration investigation becomes a criminal investigation?

If the investigation of an immigration offence develops into a criminal investigation, and if you are a competent authority processing personal data for the purposes of law enforcement, you should undertake processing under Part 3 of the DPA 2018, rather than under the UK GDPR regime. Personal data has to be

handled according to the requirements laid out in Part 3, which has its own restrictions about the rights of individuals. More information is available in our [guide to law enforcement processing](#).

Example

The Home Office is investigating an individual for an immigration offence. Investigations show that they were involved in the trafficking of individuals into forced labour in the UK. The Home Office now has to investigate under Part 3 of the DPA 2018 as a criminal offence.

Should the individual choose to exercise any of their data protection rights, the Home Office will have to consider these under the requirements of Part 3 of the DPA 2018 and apply restrictions accordingly.

National security and defence

At a glance

- In order to safeguard national security or for defence purposes there is an exemption provided for at section 26 of the DPA. It is capable of exempting personal data from most of the data protection principles and obligations, and individuals rights, where this is required to safeguard national security or for defence purposes.
- This guidance only considers the national security aspects of this exemption. In the future, the ICO will develop additional content on the defence aspects of this exemption, and will publish an amended version of this guidance in due course.
- You may be able to apply this exemption if you process data under the UK GDPR.
- This is not a blanket exemption. You must be able to show that the exemption from specified data protection standards is required for the purposes of safeguarding national security. When deciding whether to use this exemption, we suggest you consider whether complying with the UK GDPR would raise a real possibility of an adverse effect on national security.
- A Minister of the Crown (specifically a member of the Cabinet, the Attorney General or the Advocate General for Scotland) can issue a certificate which covers your processing in relation to national security. If you have decided that it is necessary to rely on the exemption, you can rely on this certificate as conclusive proof that the exemption applies. However, you should not assume that you must apply the exemption, simply because a certificate has been issued. We will publish details of relevant certificates.
- You must always have a lawful basis under Article 6, and show that your processing is more generally lawful. There is no exemption from the requirement to process lawfully.
- You must always comply with your general accountability and governance obligations.
- Modified rules apply to how you process special category data and to your security obligations.

Checklist for using the exemption

- We are not an intelligence service or a competent authority processing for law enforcement purposes.
- We are processing personal data for national security purposes, and compliance with UK GDPR rules would have implications for national security.
- We comply with the data protection principles, rights and obligations other than to the extent that an exemption is required to safeguard national security.
- We have a lawful basis for our processing, and have complied with our documentation and other accountability obligations.
- We can point to a clear link between compliance with a specific provision and a potential adverse effect on national security.
- We do not apply the exemption in a blanket manner, but only to the extent required to protect

national security.

- We have considered whether a national security certificate is applicable in the circumstances.
- We have recorded the use of the exemption and can demonstrate its necessity and proportionality in light of the data subject's rights and legitimate interests.
- We understand the special rules for special category data.

In brief

- [Does this guidance apply to us?](#)
- [What does “national security” cover?](#)
- [What is the national security exemption?](#)
- [How does the exemption work?](#)
- [When is the exemption likely to apply?](#)
- [What is a ministerial certificate?](#)
- [What are the special rules for special category data?](#)
- [How are our security obligations affected?](#)
- [What about law enforcement processing?](#)

Does this guidance apply to us?

This guidance applies to you if you usually process data under the UK GDPR, and you are carrying out processing for national security purposes.

If you are a “competent authority” processing for law enforcement purposes related to national security, different provisions apply and you should read our [Guide to law enforcement processing](#). However, if you are also processing data for a non-law enforcement purpose this guidance applies.

The intelligence services (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 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 is the national security exemption?

Section 26 of the DPA 2018 sets out a broad exemption from specified provisions of the UK GDPR:

“

“...if exemption from the provision is required for—

- (a) the purpose of safeguarding national security, or
- (b) defence purposes.”

This guidance only focuses on the national security element of this exemption.

If the exemption applies, it can exempt you from:

- any of the data protection principles (except lawfulness requirements);
- any of the rights of individuals;
- personal data breach reporting;
- international transfers requirements; and
- some of the Commissioner’s duties and enforcement powers.

You must always ensure that your processing is lawful, and that you have a lawful basis under Article 6.

If you are processing special category data for national security purposes there is no exemption from Article 9, but special rules apply. Section 28 of the DPA permits the processing of special category data for safeguarding national security, provided you ensure there are appropriate safeguards for the rights and freedoms of data subjects. For more information on this see [What are the special rules for special category data?](#) below.

If you are processing criminal offence data, and can apply this exemption, you are also exempt from your obligations under article 10 of the UK GDPR.

You must always comply with your accountability and governance obligations, including the requirement to be able to demonstrate compliance (Article 5(2) of the UK GDPR).

Although there is no exemption from security obligations, modified provisions apply to data processed for national security purposes. For more information on this see [How are our security obligations affected?](#) below.

Further reading – ICO guidance

- Lawful basis for processing
- Accountability and governance

How does the exemption work?

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

The exemption applies if it is “required” to safeguard national security. In this context, “required” means that the use of the exemption is “reasonably necessary”. This is linked to human rights standards. This means that any interference with privacy rights should be necessary and proportionate in a democratic society to meet a pressing social need.

The exemption is capable of being applied to a large number of the data protection provisions. However, it is not a blanket exemption and national security will not automatically override individual rights. You should consider your use of the exemption on a case-by-case basis.

In particular, it is not enough that the data is processed for national security purposes. You must consider the actual consequences to national security if you had to comply with the particular UK GDPR provision. If you can reasonably comply with the provision without affecting national security, you must. Of course, this is subject to any other exemptions that might apply in the specific circumstances.

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

If you use the exemption, you should be able to make a reasoned and convincing argument about the risks of compliance with the UK GDPR provisions. You may base these on hypothetical scenarios, as long as they are still realistic and credible.

For example, you may need to use the exemption to provide a consistent “neither confirm nor deny” (NCND) response about whether you process data for national security purposes. This may even be in a case where there is no direct impact on national security. This is 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.

Instead of an NCND response, you could also give a different form of non-committal response. There may be circumstances when it is not appropriate to inform a person that you are relying on the national security exemption and you may wish to word your response appropriately.

Example

An organisation is concerned that some of its service users are at risk of radicalisation from extremist groups. It passes details of individuals it considers may have been approached or are at risk to the relevant authorities.

A group of service users make subject access requests to the organisation. They ask specific questions about whether their details have ever been “passed to the authorities”. The service users have announced publicly on social media that they intend to share their responses with each other.

The organisation has informed the relevant authorities about some members of the group of service users, but not others. It is concerned that if radicalised individuals become aware that their details have been shared, it may damage national security, put lives in danger and they may take steps to thwart surveillance or other monitoring of their actions.

The organisation must respond to the subject access requests, but can use the exemption to avoid revealing any information about whether or not it has referred details to relevant authorities. It can omit the relevant details from the information it does provide. It can also provide a non-committal response to any direct question about disclosures to the authorities, regardless of whether or not the referral has in fact taken place.

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](#).

When is the exemption likely to apply?

You can use the exemption if you can show that complying with the relevant rule would be incompatible with safeguarding national security.

You can also use the exemption to maintain a consistent line so that individuals cannot draw inferences which might harm national security in other cases. For example, giving a non-committal response to subject access requests about national security processing. You do not have to confirm that you are relying on the exemption or give any details which allow an individual to infer that additional information is in fact processed.

Example

A company is concerned that some of its customers may be using its products to make bombs. It decides to provide MI5 with information about these customers and their purchases.

A customer makes a subject access request to the company for their personal data, along with details of the processing. The company should comply with the usual UK GDPR rules on the right of access in the normal way for the processing it does for its own business purposes. However, it is likely to be able to use the national security and defence exemption to avoid giving any information about the disclosures to MI5. In this case, alerting a suspected bomb-maker to the fact that MI5 is aware of their activities would clearly raise a real risk to MI5's ability to effectively safeguard national security.

If the customer makes a request for erasure of their data, the company can delete its ordinary customer records as usual but rely on the exemption to avoid deleting the data shared with MI5. It could also rely on the exemption to avoid informing the customer that it had not deleted all of the data.

You cannot use the exemption if the impact of compliance would be trivial or is not linked to national security (eg to avoid embarrassment).

You cannot use the exemption in a blanket way just because you process data for national security purposes. You must be able to show some link between compliance with the specific provision and the need to safeguard national security, even if that link is indirect. If necessary, we would expect you to be able to provide us with evidence about why you used this exemption.

What is a ministerial certificate?

Section 27 of the DPA says that a Minister 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 exemption is required for the purpose of safeguarding national security.

It is important to remember that you do not require a certificate in order to rely on the national security exemption. In fact, in most cases, controllers will determine for themselves whether they require an exemption to safeguard national security. It is also important to note that there are no certificates for relying on this exemption for defence purposes.

The exemption and the ministerial certificate do different things. The exemption, as detailed above, is always available. You may properly apply it 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 it certifies that an exemption is required for specified personal data to safeguard national security.

In this context, a ministerial certificate is admissible as conclusive evidence that exemption from the specific provision listed in section 26 is required to safeguard national security.

These certificates can be issued in advance or retrospectively. The personal data to which the certificate applies may be identified in general terms.

The ICO will publish 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 will 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 exemption applies. However, you should still consider whether you actually need to rely on the exemption, and the certificate, in a particular case. You may need to check with the relevant authorities whether or not you should rely on a certificate.

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 27. 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.

For more information on ministerial certificates, see the [Guide to intelligence services processing](#).

Further reading

[National security certificates on the ICO website](#)

What are the special rules for special category data?

Section 28 of the DPA 2018 modifies the rules on special category data for the purpose of safeguarding national security.

You may not always need to identify an Article 9 condition for that element of your processing as long as you have “appropriate safeguards” in place to protect individuals’ rights and freedoms. This reflects the substantial public interest in national security. However, you still need to ensure you have an Article 6 lawful basis for your processing.

The DPA does not specify how you can demonstrate that you have appropriate safeguards in place – so it is your responsibility to identify a reasonable way to do so.

However, one way in which you can demonstrate this is to have a document similar to the [appropriate policy document](#).

This document should briefly outline:

- how you have met the lawfulness requirements of principle (a) – including which lawful basis you are relying upon;
- your retention and deletion policies; and
- an indication of the retention period for the specific data.

If you already have an appropriate policy document for the processing of special category data, you may wish to include the details about your security processing in it.

It is good practice to retain these details until six months after the date you stop this processing. You must keep it under review. You do not have to publish it, although it is good practice to do so (although it may not be appropriate to do so for national security reasons).

How are our security obligations affected?

Section 28 also modifies the security obligations placed on a controller. So, slightly different security obligations apply if you are processing for the purpose of safeguarding national security.

You must implement security measures appropriate to the risks arising from your processing. There are also specific additional requirements for any electronic data. You must evaluate the risks, and implement specific measures to:

- prevent unauthorised processing or interference with your electronic systems;
- ensure that you can establish the details of any processing which takes place (ie there is an electronic audit trail);
- ensure proper functioning and restoration of the system; and
- ensure that data will not be corrupted if a system malfunctions.

What about law enforcement processing?

If you are a competent authority processing for law enforcement purposes, different rules apply under Part 3 of the DPA 2018.

There is no equivalent broad exemption to safeguard national security for law enforcement processing. The usual principles and obligations apply. However, there are some restrictions built-in to some of the rights of data subjects, and some of the provisions about reporting data breaches. These can apply where necessary and proportionate to protect national security. A Minister can sign a certificate as conclusive evidence that these restrictions apply, in a similar way to the UK GDPR exemption.

For more information on the restrictions available to protect national security, see the [Guide to law enforcement processing](#).

For more information on processing by the intelligence services themselves and the equivalent exemption in Part 4 of the DPA 2018, see the [Guide to intelligence services processing](#).