Your data matters: A toolkit for individuals

Advice on how to look after your personal data

YOUR DATA MATTERS

ico.
Information Commissioner's Office

The Information Commissioner's Office (ICO) oversees the laws that give you rights about the personal data organisations hold and makes sure this data is handled properly.

We have written this leaflet to give you advice and tips on how to manage and safeguard your personal data.

The leaflet will:

1. Answer some common questions about the use of your personal data

2. Explain how you can exercise your legal rights

- To be informed
- To access your data
- To access your personal data held by the police
- To get your data corrected
- To get your data deleted
- To limit how organisations use your data
- To data portability
- To object to your data being processed
- Related to automated decision-making including profiling

3. Explain what you can do if you disagree with the outcome or remain dissatisfied with a request you have made to an organisation about your rights

- Give you tips to protect your data
- Explain how to stop unwanted marketing
- Tell you how to recognise the signs of identity theft

Contents

Introduction

We live in a data-driven world. Almost every transaction and interaction you have with organisations involves sharing personal data, such as your name, address and date of birth. You share data online too, every time you visit a website, search for or buy something, use social media or send an email.

Sharing data helps makes life easier. It is more convenient and keeps us connected. We can communicate instantly. Pay bills. Book holidays. Apply for jobs. Shop and buy things effortlessly. Get dentist appointment reminders. We can even find love online. Sharing data brings countless benefits and advantages into our everyday lives.

Your data matters

Your data is central to your everyday life, so it's important it is used only in ways you would reasonably expect, and that it stays safe.

Common questions

Every organisation you have contact with holds your data. Banks, retailers and insurance companies. Music and TV streaming services. Your doctor, dentist and school. Your social media apps. The list goes on.

When your data is held and used by a number of organisations and businesses, it's completely natural for you to have questions or concerns. Here are a few:

Can I trust how organisations use my data?

All organisations and businesses using and storing personal data must follow data protection law. Your right to be informed means any organisation that wants to use your data must explain how they will use it and why. In some circumstances you also have a right to object if you don't want your data to be used or processed. If organisations do not follow data protection law you can report them to the ICO.

Can I access my personal data?

Yes. You can ask any organisation you think is holding, using or sharing your data to confirm whether it is and send you a copy of it. There may be times when an organisation withholds some of your data. However, it has to let you know it has done this and why. Read your right to access for more info.

Are organisations allowed to share my data?

Yes but in most circumstances they have to get your permission first. If an organisation does not have your permission they must have a legitimate reason for doing so. Read your right to be informed for more info.

How long do organisations hold on to my data?

Your data can only be held for the length of time it takes to fulfil the original, specified purpose – unless there is a good reason for holding it for longer. If you think your data is being held for longer than it should be, you have a right to object and a right to erasure.

How do I get my data erased?

Contact the organisation and ask them. However, you don't have an automatic right to have data deleted. There may be some reasons that mean it must still be processed, such as freedom of expression or if the organisation has to process the data to comply with another law. Read your right to erasure for more info.

How do I get data corrected?

If you think an organisation holds inaccurate data about you or something needs updating, such as your address because you've moved house, you have a right to get this changed. Read about your right to rectification for more information.

How do I question an automated decision?

Automated decision-making is when organisations use computers to evaluate data and make decisions without any human involvement. It might affect whether you're considered for a job, for example. Most of the time, automated decision-making is reliable and effective but if you have concerns, take a look at your rights related to automatic decision-making including profiling.

What are your individual rights: Right to be informed if your personal data is being used

These rights are here to give you more say and control over how your data is used.

Your right to be informed means that organisations must tell you how they'll use your data and who they'll share it with.

Here's what organisations have to be transparent and upfront about:

- Why your data is being processed and how it will be used and stored.
- Who will be responsible for your data – in other words, who the controller is and how to contact them.
- Who will see or have access to your data.
- Who else it will be shared with, if relevant.
- How long they will keep your data.
- If your data will be transferred to another country.
- If your data will be used to make an automated decision about you.
- If your data will be used to create a profile about you.
- Your right to complain.

An organisation must inform you if it is using your personal data. It should provide detailed information on:

- Why it is using your data.
- What type/types of data it is using.
- How long your data will be kept.
- Whether it is going to transfer your data to third parties, including their names and the reasons for the transfer.
- Whether it is going to transfer the data overseas, including the country involved and what will be done with the data.
- Your information rights.
- Where the data is from.
- If it is using the data in profiling (a type of automated processing where your personal data is used to analyse or predict things such as your performance at work, economic situation, health, personal preferences and interests).
- How to contact the organisation.
- Your right to complain to the ICO.

We call this 'privacy information'.

The organisation should give you privacy information at the time it collects your data. If it obtains your data from another source, it should provide privacy information within one month. It may do so in the form of a privacy notice.

This is called your 'right to be informed'.

When can an organisation not inform you of its activities?

Generally, organisations must give you privacy information, but in some circumstances they don't have to. These include where:

- you already have the privacy information and nothing has changed
- giving you the privacy information is impossible or would require "disproportionate effort", or
- giving you the privacy information would make it impossible to use your data or seriously damage the reasons for its use.

What are your individual rights: Right to access

You have the right to find out if an organisation is using or storing your personal data. This is called the right of access. You exercise this right by asking for a copy of the data, which is commonly known as making a 'subject access request'.

You're entitled to know:

- Why your data was collected and how it was processed.
- How long your data will be kept.
- Who has seen or had access to your data.
- Whether your data has been used to make an automated decision about you.
- Whether your data has been used to create a profile about you.

Your right to access means you can ask to see the data an organisation holds on you, and to verify the lawfulness of its processing. There are exceptions, but it's your right to ask if it's reasonable. In most instances, you should receive the information free of charge, and within one month. If your request is excessive, an organisation may charge a fee or refuse it, so it's best to make sure it's one you really need to make.

A letter template is available at www.ico.org.uk

How to access your data

You can make a subject access request to find out what data is held and how it is used. You may make a subject access request before exercising your other information rights.

You can make a subject access request verbally or in writing. If you make your request verbally, we recommend you follow it up in writing to provide a clear trail of correspondence. It will also provide clear evidence of your actions.

To exercise your right of access, follow these steps:

Step 1

- Identify where to send your request.
- Think about what personal data you want to access.

Step 2

- Make your request directly to the organisation.
- State clearly what you want.

You might not want all the personal data that the organisation holds about you. It may respond more quickly if you explain this and identify the specific data you want.

When making a subject access request, include the following information:

- Your name and contact details.
- Any information used by the organisation to identify or distinguish you from other people with the same name (account numbers etc).
- Any details or relevant dates that will help it identify what you want.

For example, you may want to ask for:

- your personnel file
- emails between 'A' and 'B' (between, say, 1 June 2018 and 1 Sept 2018).
- CCTV camera data situated at 'E location' on, say, 23 May 2017 between 11am and 5pm, or
- records detailing the transfer of your data to a third party.

Step 3

- Keep a copy of your request.
- Keep any proof of postage or delivery.

When should we re-submit a request?

You can ask an organisation for access more than once. However, it may be able to refuse access if your request is, as the law says, 'manifestly unfounded or excessive'.

If you are thinking of resubmitting a request, you should think about whether:

- it is likely that your data has changed since your last request
- enough time has passed for it to be reasonable to request an update on how your data is being used, or
- the organisation has changed its activities or processes recently.

What must organisations do?

If an organisation reasonably needs more information to help it find your data or identify you, it has to ask you for the information it needs. It can then wait until it has all the necessary information before dealing with your request.

When it responds to your request, the organisation should provide you with a copy of your data. It may do this electronically. If you need your data in another format, you must ask if this is possible.

You are also entitled to be told the following things:

- What it is using your data for.
- Who it is sharing your data with.
- How long it will store your data, and how it made this decision.
- Information on your rights to challenge the accuracy of your data, to have it deleted, or to object to its use.
- Your right to complain to the ICO.
- Information on where your data came from.
- Whether your data is used for profiling or automated decision-making and how it is doing this.
- If it has transferred your data to a third country or an international organisation, what security measures it took.

When can the organisation say no?

An organisation may refuse your subject access request if your data includes information about another individual, except where:

- the other individual has agreed to the disclosure, or
- it is reasonable to provide you with this information without the other individual's consent.

In deciding this, the organisation will have to balance your right to access your data against the other individual's rights regarding their own information.

The organisation can also refuse your request if it is 'manifestly unfounded or excessive'.

In any case the organisation will need to tell you and justify its decision. It should also let you know about your right to complain to the ICO, or through the courts.

How long should the organisation take?

An organisation has one month to respond to your request. In certain circumstances it may need extra time to consider your request and can take up to an extra two months. If it is going to do this, it should let you know within one month that it needs more time and why. For more on this, see our guidance on Time Limits (see page 71)

Can it charge a fee for this?

A copy of your personal data should be provided free. An organisation may charge for additional copies. An organisation can only charge a fee if it thinks the request is 'manifestly unfounded or excessive'. If so, it may ask for a reasonable fee for administrative costs associated with the request.

Get access to your personal data held by the police

The right of access allows you to obtain personal information held about you by organisations, including police forces and the wider criminal justice system.

How to make your request

You should normally make your request to your local police force. They will be able to access information held about you centrally, most notably through the PNC (Police National Computer). If you no longer live in the UK, contact the police force for the area where you last lived.

If you have been in contact with the police because you were a witness or victim, or because of a traffic accident, then this information may not be available to other police forces. In these cases you should contact the police force you dealt with at the time.

Although you don't have to use them, police application forms will help you understand what details you need to provide so they can find the information you have requested. It will also outline what proof of ID they will need to see. For example, they may ask you when you have been in contact with the police and why, and whether you have lived in another part of the UK. You can make a request verbally or in writing. If you make your request verbally, we recommend you follow it up in writing to provide a clear trail of correspondence. It will also provide clear evidence of your actions.

To exercise your right of access, follow these steps:

Step 1

- Identify where to send your request.
- Think about what personal data you want to access.

Step 2

- Make your request directly to the organisation.
- State clearly what you want.

You might not want all the personal data that the organisation holds about you. It may respond more quickly if you explain this and identify the specific data you want.

When making an access request, include the following information:

- Your name and contact details.
- Any information used by the organisation to identify or distinguish you from other people with the same name (account numbers etc).
- Any details or relevant dates that will help it identify what you want.

For example, you may want to ask for:

- your interview statements;
- Footage of you captured through CCTV/other recordable devices
- custody records; and
- correspondence between the police and other organisations, such as those providing support to you.

What are your individual rights: Right to to get your data corrected

If your personal data is incorrect or out of date, then there can be severe repercussions for you. Sometimes mistakes can simply happen, and errors or inaccuracies creep in. Your right to rectification entitles you to have your data corrected.

The organisation has to respond within one month. Or three months, maximum, if there are complexities to deal with. In most cases, you won't be charged. Also, if incorrect data has been shared with other organisations, it's the original organisation's responsibility to pass on the updated info.

You can challenge the accuracy of personal data held about you by an organisation, and ask for it to be corrected or deleted. This is known as the 'right to rectification'. If your data is incomplete, you can ask for the organisation to complete it by adding more details.

How to get your data corrected

To exercise your right to rectification you should inform the organisation that you are challenging the accuracy of your data and want it corrected. You should:

- state clearly what you believe is inaccurate or incomplete
- explain how the organisation should correct it, and
- where available, provide evidence of the inaccuracies.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

What about data that records a mistake?

It can be complex to decide whether data is inaccurate if it refers to a mistake that has then been put right. An organisation could argue that the fact the mistake was made is an accurate thing to record, so it should record the mistake alongside the correct data.

> **Example**: A doctor finds that a patient has a particular illness and notes it in their medical records. Sometime later, this diagnosis is found to be wrong. It is likely that the medical records should include both the initial diagnosis and the final findings because this gives 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 corrected.

What about data that records an opinion?

It is also complex if the data in question records an opinion. Opinions are, by nature, subjective. As long as the record is clear that the data is an opinion and, where appropriate, whose opinion it is, it can be difficult to maintain it is inaccurate and needs to be corrected.

What must organisations do?

When an organisation is asked to correct data, it should take reasonable steps to investigate whether the data is accurate, and should be able to demonstrate it has done so. To do this it should consider your arguments and any evidence you provide.

The organisation should then contact you and either:

- confirm it has corrected, deleted or added to the data, or
- inform you it will not correct the data, and explain why it believes the data is accurate.

If the organisation has disclosed the data to others, it must contact them and tell them the data has been corrected or completed – unless this is impossible or involves a disproportionate effort. When asked, the organisation must inform you which recipients have received the data.

Can organisations refuse to carry out the request?

Yes, but only in certain circumstances. If the organisation refuses to correct the data, as a matter of good practice it should record that you have challenged the data's accuracy and why.

The organisation can also refuse to comply with a request for rectification if it believes that the request is what the law calls 'manifestly unfounded or excessive'. In reaching this decision, it can take into account whether the request is repetitive.

In such circumstances the organisation can:

- request a reasonable fee to deal with the request, or
- refuse to deal with the request.

In either case it will need to tell you and justify its decision.

How long should the organisation take?

An organisation has one month to respond to your request. In certain circumstances it may need extra time to consider your request and can take up to an extra two months. If it is going to do this, it should let you know within one month that it needs more time and why. For more on this, see our guidance on Time Limits (see page 71).

Can the organisation charge a fee?

An organisation can only charge a fee if it thinks the request is "manifestly unfounded or excessive". If so, it may ask for a reasonable fee for administrative costs associated with the request.

What are your individual rights: Right to get your data deleted

Your right to erasure means you can ask for your data, such as photographs, to be removed. It may not always be possible but if it's your data, it's your right to ask.

You may sometimes hear this called the 'right to be forgotten'.

You can ask for your data to be erased, if:

- The organisation no longer needs your data.

  Example: after you have cancelled your gym membership, it no longer needs to keep details of your name, address, age and health conditions.

- You initially consented to the use of your data, but have now withdrawn your consent.

  Example: you agreed to take part in a market-research study and now no longer wish to do so.

- You have objected to the use of your data, and your interests outweigh those of the organisation using it.

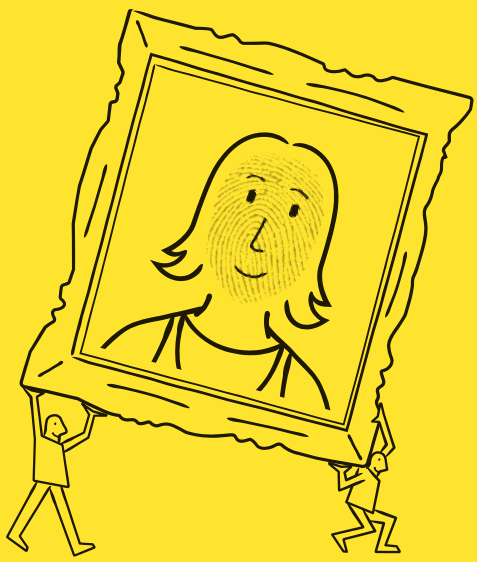
For more, read 'Your right to object to how your data is used' (See page 40).

- The organisation has collected or used your data unlawfully.

  Example: it hasn't complied with the rules on data protection.

- The organisation has a legal obligation to erase your data.
- The data was collected from you as a child for an online service.

  Example: social media or a gaming app.



How do you ask for your data to be deleted?

You should contact the organisation and let it know what you want erased. You don't have to ask a specific person – you can contact any part of the organisation with your request.

You can make a request verbally or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

When can you request erasure?

The right to erasure is not absolute. The right only applies in the following circumstances listed above.

The law gives children special protection because they may be less aware of the risks and consequences of giving their data to organisations. Even if you are now an adult, you have a right to have your data erased if it was collected from you as a child.

What should the organisation do?

The organisation should delete your data. It should also inform anyone else it has shared your data with about the erasure. It can only refuse to do this if it would be impossible or involve disproportionate effort. It must also inform you of the fact it has shared your data with these other people, if you ask.

If your personal data has been made public in an online environment – such as on social networks, forums or websites – then the organisation must take reasonable steps to inform the people with responsibility for these sites about the erasure.

When can the organisation refuse a request?

The organisation can refuse to erase your data in the following circumstances:

- When keeping your data is necessary for reasons of freedom of expression and information (this includes journalism and academic, artistic and literary purposes).
- When it is legally obliged to keep hold of your data.
- When keeping hold of your data is necessary for reasons of public interest in the area of public health.
- When processing it is necessary for the purposes of scientific or historical research, or archiving that is in the public interest, and the erasure would impair these objectives.
- When keeping your data is necessary for establishing, exercising or defending legal claims.

The organisation can also refuse your request if it is, as the law states, 'manifestly unfounded or excessive'.

If, having considered your request, the organisation decides it does not need to erase your data, it must still respond to you. It should explain to you why it believes it does not have to erase your data, and let you know about your right to complain about this decision to the ICO, or through the courts.

How long should the organisation take?

An organisation has one calendar month to respond to your request. In certain circumstances it may need extra time to consider your request and can take up to an extra two months. If it is going to do this, it should let you know within one month that it needs more time and the reasons why. For more on this, see our guidance on Time Limits (see page 71).

The organisation might need you to prove your identity. However, it should only ask you for just enough information to be sure you are the person whose data it holds. If it does this, the one-month time period to respond to your request begins from when it receives this additional information.

Can it charge a fee?

In most circumstances, no. An organisation can only charge a fee if the request is "manifestly unfounded or excessive". It may then ask for a reasonable fee for administrative costs associated with your request.

What are your individual rights: Right to limit how organisations use your data

You have the right to limit the way an organisation uses your personal data. You may want a restriction placed on the data because you have concerns over its accuracy or how it is being used. In other circumstances requesting a restriction can be used to prevent an organisation from deleting it.

You can use your right to restrict if:

- You've used your right to rectification and want your data to be left alone while the organisation is checking it's correct and up to date.
- The use of your data is unlawful but you don't want it deleting.
- There's no longer any need for the organisation to use your data, but you need it to assist with something, e.g. a legal issue, so you want the data kept
- You have used your right to object to the use of your data, and the organisation is considering this.

You can limit the way an organisation uses your personal data if you are concerned about the accuracy of the data or how it is being used. If necessary, you can also stop an organisation deleting your data. Together, these opportunities are known as your 'right to restriction'.

This right is closely linked to your rights to challenge the accuracy of your data and to object to its use (see page 40).

How you can ask an organisation to restrict the use of your data

To exercise your right to restriction, you should:

- make your request directly to the organisation, and
- say what data you want restricted and why.

If you want to, you can make a request for restriction at the same time as you raise another objection.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

When you can ask an organisation to restrict the use of your data

You can ask organisations to temporarily limit the use of your data when they are considering:

- a challenge you have made to the accuracy of your data, or
- an objection you have made to the use of your data.

You may also ask an organisation to limit the use of your data rather than delete it if:

- the organisation processed your data unlawfully but you do not want it deleted, or
- the organisation no longer needs your data but you want the organisation to keep it in order to create, exercise or defend legal claims.

What must the organisation do?

The organisation must take appropriate steps to restrict the use of your data. These could include:

- temporarily moving your data to another system
- making it unavailable to users, or
- temporarily removing it from a website, if it has been published.

If the organisation has shared the data with others, it must contact each recipient and inform them of the restriction – unless this is impossible or involves a disproportionate effort. It must also inform you about these recipients if you ask.

When can an organisation use restricted data?

The organisation should store the restricted data securely and should not use the data unless:

- it has your consent to do so
- the data is needed for legal claims
- its use is to protect another person's rights, or
- its use is for reasons of important public interest.

Once the organisation has investigated your complaint, it may decide to lift the restriction and continue using your data. You should be informed before the restriction is lifted.

When can the organisation say no?

If it believes that a request is, as the law states, "manifestly unfounded or excessive", an organisation can:

- request a reasonable fee to deal with the request, or
- refuse to deal with the request.

In either case it will need to tell you and justify its decision.

How long should the organisation take?

An organisation has one calendar month to respond to your request. In certain circumstances the organisation may need extra time to consider your request and can take up to an additional two months. If it is going to do this, it should let you know within one month that it needs extra time and the reason why. For more information, see our guidance on Time Limits (see page 71).

Can it charge a fee for this?

An organisation can only charge a fee if the request is "manifestly unfounded or excessive". It may then ask for a reasonable fee to cover administrative costs associated with the request.

What are your individual rights: Right to data portability

You can move your personal data easily and securely from one service or provider to another, or to yourself. Doing this may help you find a better deal, or better understand your spending habits.

Some organisations already offer this service, making it easy to copy across contacts and music, for example, to another service. You should get a response from the organisation within one month. Or if it is complex, they make take two more months.

You have the right to get your personal data from an organisation in a commonly-used, machine-readable format, for example a CSV file. You also have the right to ask an organisation to transfer your data to another organisation if it is technically feasible to do so.

This is known as the right to data portability.

What kind of data does this right relate to?

This right is similar to your right of access (see page 12) but there are some differences. Specifically, the right only applies:

- to data that is held electronically, and
- where you have provided it to the organisation.

Data you have provided does not just mean information you have typed in, such as a username or email address. It may include data the organisation has gathered from monitoring your activities when you have used a device or service. This may include:

- website or search usage history
- traffic and location data, or
- 'raw' data processed by connected objects such as smart meters and wearable devices. An example of this could be data recorded on a fitness app.

When can you make a portability request?

You can make a portability request at any time to any organisation that:

- relies on your consent (see page 72) to use your personal data, or
- uses your data as part of a contract you have with them.

The organisation's privacy notice will tell you more about why it is using your data.

How do you make a data portability request?

To exercise your right to portability you should:

- make your request directly to the organisation; and
- state what you want.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

What must an organisation do?

The organisation must provide a copy of the requested data in a structured, commonly used, machine-readable format, such as a CSV file. The organisation may also allow you to access the data yourself through an automated tool.

Depending on the nature of your request, the organisation should either send the data to you or to an organisation you have identified. Before doing this, the organisation may need to confirm your identity.

The organisation does not have to automatically delete your data after giving it to you or sending it to another organisation. So if you want your data to be deleted, you also may need to exercise your right to erasure (see page 24).

When can an organisation refuse?

If the organisation believes that a request is "manifestly unfounded or excessive", it can:

- request a reasonable fee to deal with the request, or
- refuse to deal with the request.

In reaching this decision, it can take account of whether the request is repetitive. In either case it will need to tell you and justify its decision.

If you disagree with the decision read the guidance on page 50.

How long should an organisation take?

The organisation has one month to respond to your request.In certain circumstances it may need extra time to consider your request and can take up to an extra two months to do so.

If it is going to do this, it should let you know within one month that it needs more time and why. For more on this, see our guidance on Time Limits (see page 71).

What are your individual rights: Right to object

Organisations use and process your data for lots of reasons. Sometimes, this can mean receiving marketing you don't want. In this case, it's your right to object.

You can use your right to object in these circumstances:

- for a task carried out in the public interest
- for its legitimate interests
- for scientific or historical research, or statistical purposes, or
- for direct marketing.

You have the right to object to the processing (use) of your personal data in some circumstances. If an organisation agrees to your objection, it must stop using your data for that purpose unless it can give strong and legitimate reasons to continue using your data despite your objections.

You have an absolute right to object to an organisation using your data for direct marketing – in other words, trying to sell things to you. This means it must stop using the data if you object.

How do you exercise your right to object?

Before objecting you may need to ask the organisation why it is processing your data. This is because you can only object to processing when the organisation is using your data for the reasons listed above.

What it tells you about why it is processing your personal data will show whether you can object.

If you're able to object, you should inform the organisation directly that you object to any more processing of your data. You need to set out in your objection why you believe the organisation should stop using your data in this way.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

What must the organisation do?

If your objection is successful, the organisation must stop processing your personal data for the use you have objected to. However, it may still be able to legitimately continue using your data for other purposes.

When can the organisation refuse?

The organisation can refuse to comply with your objection if it can prove it has a strong reason to continue processing your data that overrides your objection. It can also refuse if it can prove that the use of your data is for a legal claim. It should inform you of this outcome.

The organisation can also refuse to comply if it believes that your objection is, as the law states, "manifestly unfounded or excessive". In reaching this decision, it can take into account whether your objection is repetitive.

In such circumstances the organisation can:

- Request a reasonable fee to deal with the request, or
- refuse to deal with the objection.

In either case it will need to tell you and justify its decision.

How long should the organisation take?

The organisation has one month to respond to your objection. In certain circumstances it may need extra time to consider it and can take up to an extra two months. If it is going to do this, it should let you know within one month that it needs more time and why. For more on this, see our guidance on Time Limits (see page 71).

Can it charge a fee for this?

An organisation can only charge a fee if the objection is "manifestly unfounded or excessive". It may then ask for a reasonable fee to cover administrative costs associated with your objection.

What are your individual rights: Rights on automatic decision-making and profiling

Automatic decision-making is when an algorithm analyses your personal data – rather than a human being – in order to make decisions about you. Most of the time, this is a quick and reliable method. But because automated systems like this don't deal in nuances and can't read between the lines, it can lead to decisions being made that don't seem right, or that you don't agree with.

If you believe that the automated processing of your personal data has disadvantaged you, you can ask for a person to review the decision. It may not always be possible but if it's your data, it's your right to ask.

When decisions are made about you without people being involved, this is called 'automated individual decision-making and profiling' or 'automated processing', for short.

In many circumstances, you have a right to prevent automated processing.

This guidance describes your rights under two kinds of automated processing:

- automated individual decision-making, and
- profiling.

What is automated decision-making?

This refers to decisions made without any human involvement, for example:

- an online decision after you have applied for credit, or
- a recruitment aptitude test using pre-programmed algorithms and criteria.

What is profiling?

Profiling means your personal data is used to analyse or predict such things as:

- your performance at work
- your economic situation, or
- your health, personal preferences and interests.

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

Profiling occurs in some automated individual decision-making.

Profiling information can be gathered from various sources, such as internet searches, buying habits, social networks and lifestyle data from mobile phones.

What are your rights regarding automated decision-making and profiling?

You have the right:

- not to be subject to a decision that is based solely on automated processing if the decision affects your legal rights or other equally important matters (e.g. automatic refusal of an online credit application, and e-recruiting practices without human intervention)

- to understand the reasons behind decisions made about you by automated processing and the possible consequences of the decisions, and
- to object to profiling in certain situations, including for direct marketing (see page 40).

How do you exercise your rights?

Organisations must not make decisions based solely on automated processing if the decision affects your legal rights or other equally important matters unless the decision is:

- necessary for the purposes of a contract between you and the organisation
- authorised by law (eg to prevent fraud or tax evasion), or
- based on your explicit consent (see page 72).

So you should not have to request them to stop. However, you do have the right at any time to ask an organisation not to subject you to automated processing in the three circumstances described above. You can also ask them to tell you why a decision has been made in this way and how it will affect you.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

What must the organisation do?

Organisations must let you know if they are carrying out automated processing and tell you what information they are using. They should give you relevant information about the reasoning involved in the decision-making as well as the expected consequences for you. You should be given real examples of the type of possible effects.

Organisations should make sure they only carry out automated processing that affects your legal rights (or any other equally important matter) if it is:

- necessary for the purposes of a contract between you and the organisation
- authorised by law (for example, to prevent fraud or tax evasion), or
- based on your explicit consent.

Where an organisation is allowed to make decisions based solely on automated processing, it should offer simple ways for you to:

- express your view on the decision
- get an explanation of the decision
- request human intervention in the decision-making process, and
- challenge a decision.

It must also tell you about the circumstances in which you can object to profiling.

If you have asked an organisation not to make an automated decision, it should tell you in writing whether or not it agrees with you and give reasons.

How long should the organisation take?

An organisation has one month to respond to your request not to be subject to an automated decision. In certain circumstances, it may need more time to consider your request and can take up to an extra two months. If it's going to do this, it should let you know within one month that it needs more time and why. For more on this, see our guidance on Time Limits (see page 71).

Can the organisation charge a fee?

In most circumstances, no. An organisation can only charge a fee if the request is, as the law states "manifestly unfounded or excessive". If this is the case, the organisation may ask for a reasonable fee for costs associated with the request.

Your right to make a complaint if you disagree with an outcome or remain dissatisfied.

If you are unhappy with how the organisation has handled your request, you should first complain to it.

Here are some tips to follow when you raise your concern.

- Raise your concern quickly. People move on, memories fade and records are deleted in line with retention policies. The longer it takes to raise your concern with an organisation, the harder it will be for them to look into it thoroughly.
- Send it to the right place. There's no point in raising a matter quickly if it then takes weeks to get to the right department. Check the organisation's website or give them a call to make sure you have the right address. In some cases, you may be able to find it on our Register of fee payers.
- Write legibly. Typed documents are easiest to read. If you write your complaint by hand, make sure your writing is easy for others to understand.
- Keep your language simple. Although you might have checked our website to see what the relevant legislation says, don't feel you have to quote it to raise a complaint. Just explain clearly and simply what has happened and, where appropriate, the effect it has had on you.
- Be specific. If you have had a long relationship with the organisation concerned, resist any temptation to include historical or unrelated complaints in your letter. This can confuse matters and leave the organisation unsure which of your concerns you really want them to deal with.
- Don't move the goalposts. Include full details of your concern at the beginning. If the organisation responds properly, don't raise additional unrelated matters as part of that complaint. However, if it appears that the organisation has misunderstood you, or has not given a full response, you should let them know.

- Stay reasonable. You may be justifiably angry or upset about what has happened. Keeping your letter calm and polite will help you get your points across more clearly. Remember that the person you are dealing with might have had nothing to do with the problem you had. Also, remember that they are only human. A rude letter might make it difficult for them to want to help.
- Don't get personal. Don't insult members of the organisation's staff. Apart from being unreasonable behaviour, the response may lack focus if the writer feels obliged to defend his or her colleagues or staff.
- Request and respect timescales. Ask when you can expect the organisation to respond and resist any temptation to contact them again before that. However, if you do not receive a response on time, you should chase it, although we recommend giving an extra couple of days to allow for administrative or postal delays.
- Include all necessary information. Include all relevant details such as account or patient numbers to help the organisation identify you and your concern correctly.
- Include all necessary evidence. Send copies of all the key documents you have to evidence your complaint. Don't send the originals as you might need them later. Also, don't include additional documentation 'just in case'. The more documents you send, the more likely it is that key information will be missed.
- Keep good records. Clearly date all letters, make notes of all related conversations and keep copies of everything.
- Exhaust the process. If the 'final' response you receive does not resolve the matter to your satisfaction but also signposts you to any further complaints or review procedure, make sure you exhaust that process before bringing the matter to our attention.

There is a template letter on the ICO's website: www.ico.org.uk

Having raised the issue with the organisation, if you remain dissatisfied you can make a complaint to the ICO on our website ico.org.uk/make-a-complaint or by calling our helpline on **0303 123 1113** (local rate – calls to this number cost the same as calls to 01 or 02 numbers).

You can also seek to enforce your rights through the courts. If you decide to do this, we strongly advise you to seek independent legal advice first.

How you can protect your personal data?

Your personal data is valuable, so you should treat it just as you would any valuable item. As data-related issues increase, it is even more important for you to safeguard your information.

Always think about who you are giving your data to. Be cautious about providing any personal details to unsolicited callers by phone, fax, post, email or in person, unless you are sure the person is who they say they are. If you are suspicious, ring the organisation back on an advertised number or visit their website. Even if you know who is asking for your data, think twice before you answer their questions.

Here are some other simple steps you can take to safeguard your data.

Paper documents and letters

- Store in a safe place any documents carrying your personal details, such as your passport, driving licence, bank statements and utility bills.
- Shred or destroy personal documents you are throwing away such as bills, receipts, bank or credit-card statements and other documents that show your name, address or other personal details.
- If you have to post personal documents, ask the post office for advice on the most secure method.
- Limit the number of documents you carry around that contain your personal details. If possible, don't leave personal documents in your vehicle.
- If you use a central or communal postal delivery point, such as in a block of flats, make sure you have a lockable postbox and collect your post as soon as possible. If your mail regularly fails to arrive, report this to Royal Mail.

If you move house, redirect all your mail and inform your bank, utility companies and other organisations of your new address. You can find more information on safeguarding your mail on page 66.

Financial information

- Check your bank and credit card statements regularly for unfamiliar transactions.
- Regularly get a copy of your personal credit file to check for any suspicious credit applications. For more information on how to do this, see our website www.ico.org.uk or ring 0303 123 1113 for a free copy of our 'Credit explained' guide.

Online, computers and WiFi

- Make sure your home computer is protected before you go online.
- You should also make sure that your device is up-to-date with the latest security patches, and that any application you use to go online (e.g. your web browser) is also up-to-date. In some cases, your applications and operating systems will have automatic update options meaning that you don't have to take any direct action yourself, aside from checking that the update function is working properly.
- Use different passwords for different accounts, and making use of two-factor authentication where it is available. Take extra care when using public computers to access your personal data.
- Take care when providing your personal data online. In particular, do not make too much personal data available to lots of people, for example by having open access on social networking sites. For further information, visit the online safety pages at our website www.ico.org.uk.
- Your personal data can be used to steal your identity and commit fraud. Be wary of anyone who asks for your bank or credit card details, and only use secure sites when shopping online – secure sites usually carry the padlock symbol 🔒.
- Secure your WiFi. An unsecured wireless network is open to hackers to gain access to your personal data.
- When you buy a wireless router, or if you already have a wireless network installed, make sure you protect yourself by enabling its security features.
- Do not click on links to go to a website unless you can be confident it is genuine.

We have further information on online safety on our website https://ico.org.uk/your-data-matters/online/

Reduce unwanted, sales calls, junk mail and electronic marketing

All organisations have to provide you with privacy information that clearly tells you how they intend to use your data. They also have to state the lawful basis for using your data. If an organisation relies on consent to send you direct marketing they have to separate the consent request from the other privacy information. They also have to ask you to perform a positive action to give your consent, such as ticking a box.

If an organisation is sharing your data with third parties, so they can use your data for marketing, they need to tell you this and those other organisations must be named.

You always have the right to ask an organisation to stop using your personal data for marketing, just follow the guidance on your right to object on page 40.

Reducing sales calls

To reduce the number of unwanted sales calls, register your home and mobile phone numbers with the Telephone Preference Service (TPS). This service is free and takes 28 days to become active. Note that registering your mobile number with the TPS will only stop live marketing voice calls, not SMS text messages, or automated calls.

To stop unwanted sales calls, register your details: online at tpsonline.org.uk; by phoning 0845 070 0707; or by writing to:

The Telephone Preference Service (TPS)
DMA House
70 Margaret Street
London
W1W 8SS

If you have a business, you can also register your company's phone number(s) with the Corporate Telephone Preference Service (CTPS). For more data on how to do this, visit www.tpsonline.org.uk/tps/whatiscorporatetps.html.

Reducing the number of silent calls

Silent calls do not fall under the Privacy and Electronic Communications Regulations as no marketing message is sent. For further advice about the rules on silent calls contact Ofcom on 020 7981 3040 or visit www.ofcom.org.uk.

Reducing the amount of fax marketing

As an individual or a business, you can also register your fax number with the Fax Preference Service to reduce the number of unwanted faxes you get. Again, this service is free, and can be done: online at fpsonline.org.uk; by phoning 0845 070 0702; or by writing to:

Fax Preference Service (FPS)
DMA House
70 Margaret Street
London
W1W 8SS

Who do I contact if I have difficulty stopping unwanted calls and faxes?

If, after you register with the TPS and FPS, you still continue to receive unwanted sales calls, visit our website www.ico.org.uk or contact our helpline on 0303 123 1113 for advice on what to do next.

Reducing direct and junk mail

To reduce the volume of unwanted direct or junk mail, register your name and address with the Mailing Preference Service (MPS). The MPS is a free service set up by the direct marketing industry to help people who don't want to receive junk mail. The MPS can remove your name and address from up to 95% of direct-mail lists. However, it will not stop direct mail from companies who don't check their list with the MPS before sending direct mail, and it won't stop mail addressed to 'the occupier'. It will take up to four months for the service to take full effect, but you should notice a reduction of mail during this period. To stop direct and junk mail: register your details online at www.mpsonline.org.uk; phone 0845 703 4599; or write to:

Mailing Preference Service (MPS)
DMA House
70 Margaret Street
London
W1W 8SS

You can also stop the amount of 'unaddressed mail' you receive by registering your address with the Royal Mail's Door to Door opt-out service. However, this service will not stop mail addressed to 'the occupier'.

To register write to:

Freepost RSTR-YCYS-TGLJ
Royal Mail Door to Door Opt Outs
Kingsmead House
Oxpens Road
Oxford
OX1 1RX

Or email:
optout@royalmail.com

Who do I contact if I have difficulty stopping unwanted mail?

If you have registered with the MPS but are still receiving unwanted mail, you can complain directly to the MPS, who will investigate and contact the company sending the mail. To complain, write to the MPS with a copy of the unwanted mail you have been sent, including the envelope, as this will help the MPS to identify the source of the mailing.

To complain, write to:

Mailing Preference Service
MPS Freepost LON20771
London
W1E 0ZT

If, after you register and complain to the MPS, you still continue to receive unwanted mail you should contact the company directly to complain. If after that they keep on sending you unwanted mail, visit our website www.ico.org.uk or contact our helpline on 0303 123 1113 for advice on what to do next.

Spam

Spam is email you don't want and didn't ask for, and its content can often cause embarrassment and distress. Most spam comes from outside the UK.

As a lot of spam comes from overseas, the Information Commissioner has an agreement with a number of overseas bodies to cooperate and exchange data to try and stop spam emails that are sent from those places. To try to reduce the amount of spam you receive, you could speak to your internet service provider (ISP) for advice on spam filters, or visit our website www.ico.org.uk for more advice on spam.

You can take the following steps to reduce the amount of spam you receive:

- Be careful who you give your email address to.
- Consider having separate personal and business email addresses.
- Choose an email address that is difficult to guess.
- Don't advertise your email address.
- Check privacy information and marketing opt-outs carefully.
- Never respond to spam. Replying can indicate your email address is live. This can encourage the more unscrupulous senders to send you even more emails.
- Don't click on the adverts in spam emails. By clicking on spammers' web pages, you identify your email address as being live and may make yourself a target for more emails. It can also make your computer open to virus and other malicious attacks.
- Use a spam filter. Spam filters are programs that work with your email package to sift through new emails, identifying spam and blocking it.

Electronic marketing

Electronic marketing includes any text, sound or picture messages organisations send you electronically.

Organisations which send you marketing using electronic methods must ask for your permission before they send it. This could be when they collect your data. In every marketing email, text or recorded message they send you, they must give you the chance to opt out.

Who do I contact if I have difficulty reducing the amount of electronic marketing I receive?

If, after you tell the organisation you no longer to want to receive electronic marketing from them and you continue to get unwanted electronic marketing, visit our website www.ico.org.uk or contact our helpline on 0303 123 1113 for advice on what to do next.

Recognising the signs of identity theft

Your identity is one of your most valuable assets. If your identity is stolen, you can lose money and may find it difficult to get loans, credit cards or a mortgage.

Your name, address and date of birth provide enough information to create another 'you'. An identity thief can use a number of methods to find out your personal information and will then use it to open bank accounts, take out credit cards and apply for state benefits in your name.

What signs should I look out for?

There are a number of signs to look out for that may mean you are or may become a victim of identity theft:

- You have lost or have important documents stolen, such as your passport or driving license.
- Mail from your bank or utility provider doesn't arrive.
- Items that you don't recognise appear on your bank or credit card statement.
- You apply for state benefits, but are told you are already claiming.
- You receive bills or receipts for goods or services you haven't asked for.
- You are refused financial services, credit cards or a loan, despite having a good credit rating.
- You receive letters in your name from solicitors or debt collectors for debts that aren't yours.

How do I reduce the risk of identity theft?

- Store any documents carrying personal information – such as your driving license, passport, bank statements, utility bills or credit card transaction receipts – in a safe and secure place.
- Shred or destroy your old documents so that nothing showing your name, address or other personal details can be taken.
- Monitor your credit report and regularly check your credit card and bank statements for suspicious activity.
- When you move house, contact your bank, credit and store card providers, mobile phone provider, utility providers, TV licensing, your doctor and dentist etc, and give them your new address – you don't want the new tenants to have access to letters containing your personal information. You can also redirect your mail by contacting Royal Mail.
- Remember, less is more. The less you give away about yourself, the lower the risk of information falling into the wrong hands.
- Think before you buy online – use a secure website which displays the company's contact details, look for a padlock symbol 🔒 and a clear privacy and returns policy. Check the web address begins with https.

What can I do if I'm a victim of identity theft?

If you think you are a victim identity theft or fraud, act quickly to ensure you are not liable for any financial losses.

- Report all lost or stolen documents, such as passports, driving license, credit cards and cheque books to the organisation that issued them.
- Inform your bank, building society and credit card company of any unusual transactions on your statement.

- Request a copy of your credit file to check for any suspicious credit applications.
- Report the theft of personal documents and suspicious credit applications to the police and ask for a crime reference number.
- Contact CIFAS (the UK's Fraud Prevention Service) to apply for protective registration. Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.

  CIFAS – The UK's Fraud Prevention Service
  6th Floor
  Lynton House
  7 - 12 Tavistock Square
  London
  WC1H 9LT
  www.cifas.org.uk

You can also get more advice at:

- Action Fraud
  www.actionfraud.police.uk
- Bank Safe Online
  www.banksafeonline.org.uk
- Financial Ombudsman Service
  Telephone: 0800 0 234567
  www.financial-ombudsman.org.uk
- CardWatch c/o APACS
  Mercury House
  Triton Court
  14 Finsbury Square
  London EC2A 1LQ
  www.cardwatch.org.uk

To report the theft or loss of post and other important documents:

- Royal Mail
  Telephone: 08457 740 740
  www.royalmail.com

If you would like to contact us please call 0303 123 1113 www.ico.org.uk Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Glossary

Here's a quick guide to some data protection terminology.

Your personal data

Personal data is anything that makes you directly or indirectly identifiable, for example, your name, address and birth date. It can be automated personal data or data held in manual filing systems.

Special category data

Special category data is data about your race, ethnicity, political opinions, religious or philosophical views, trade union membership, health, sex life, genetic data and biometric data (where this is used to uniquely identify you). It doesn't include criminal convictions and offences but these do have strict safeguards around them.

Privacy notice

This is the area of an organisation's website where they clearly explain what personal data they want to obtain from you, what they want to do with it, and what measures they use to keep your data safe. The data controller's contact details should also be listed here.

Processing

'Processing' broadly includes collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, combining, restricting, erasing or destroying personal data.

Calendar month

A calendar month starts on the day after the organisation receives the request, even if that day is a weekend or public holiday. It ends on the corresponding calendar date of the next month.

Example: An organisation receives a request on 3 September. The time limit starts from the next day, 4 September. This gives the organisation until 4 October to comply with the request. However, if the end date falls on a Saturday, Sunday or bank holiday, the calendar month ends on the next working day.

However, if the end date falls on a Saturday, Sunday or bank holiday, the calendar month ends on the next working day.

Example: An organisation receives a request on 24 November. The time limit starts from the next day, 25 November. The corresponding calendar date is 25 December, but 25 December and 26 December are bank holidays. So the organisation would therefore have until the next working day, 27 December if that was a week day.

Also, if the corresponding calendar date does not exist because the following month has fewer days, it is the last day of the month.

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

However, if 30 April falls on a weekend, or is a public holiday, the calendar month ends the next working day.

Consent

Organisations using consent to process data must tell you what they are doing and give you the chance to say yes. This means you may see an opt-in box at the time your data is collected. The box should not be pre-ticked as you should be active in providing consent.

Your consent should be freely given and unconditional. Where there is a power imbalance, such as if the organisation is your employer or a potential employer it must make sure your consent is valid. You should not be punished for refusing to consent.

Some data processing activities are complicated. An organisation may want to undertake several processing activities with the data it collects from you. It should provide separate clear consent options so that you can tailor how your data is used.

> **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. If it provides several functions as part of its alumni service, and is processing data using consent, it may ask for consent by activity.

Organisations that process your personal data for direct marketing activities will probably be using consent as their lawful basis. This is because you have the right to determine how your personal data is used and whether you want to be marketed to.

An organisation is asking for consent but if I refuse they will not provide the service.

The collection of your consent should be separate from other terms and conditions. You should not be prevented from a service if you refuse to provide consent for data processing. It may be that the organisation actually requires your details in order to provide a product, such as undertaking a credit reference check. In this instance it is actually processing your data as part of a contract and should not be presenting this as a consent based service.

ico.

Information Commissioner's Office