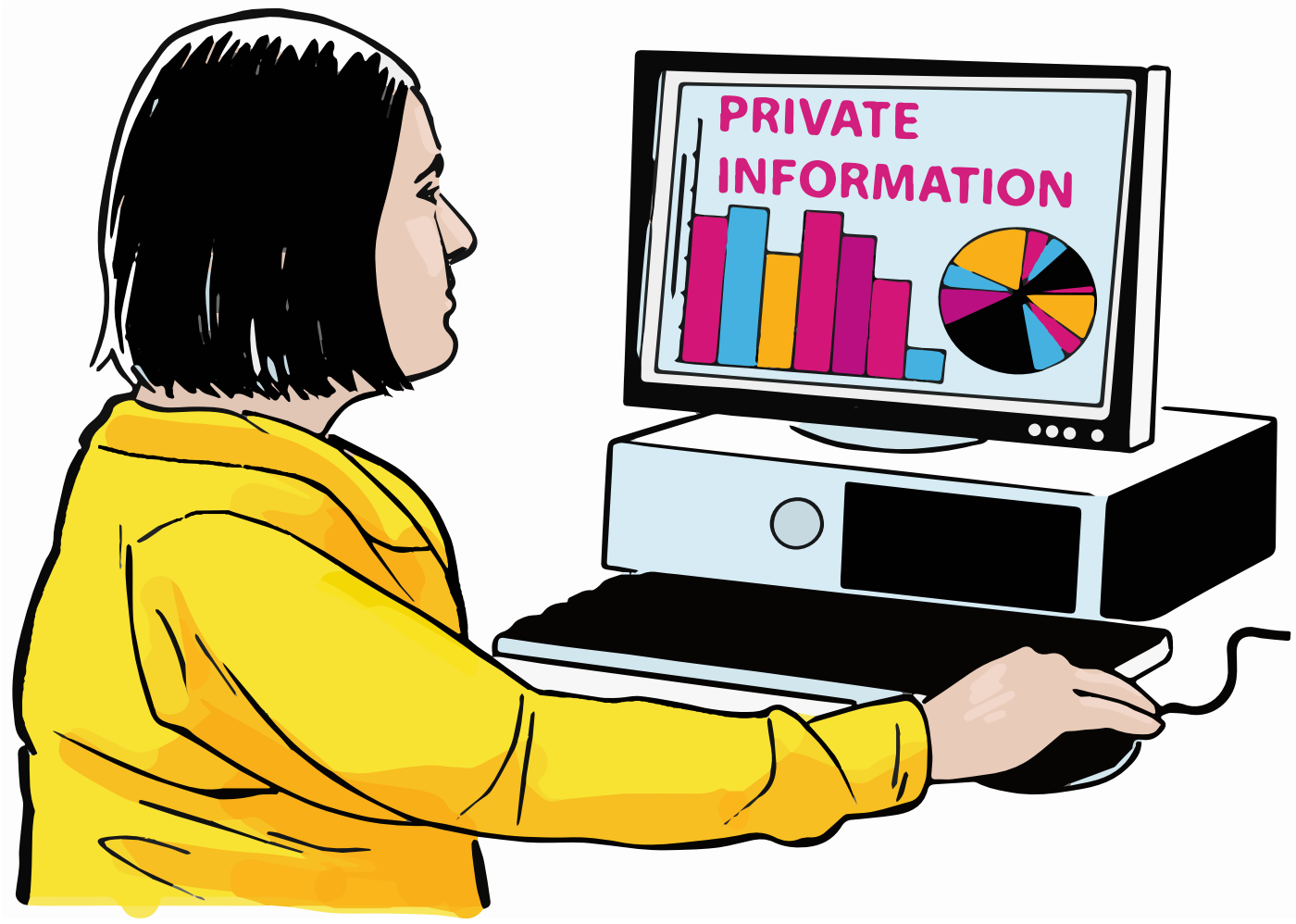
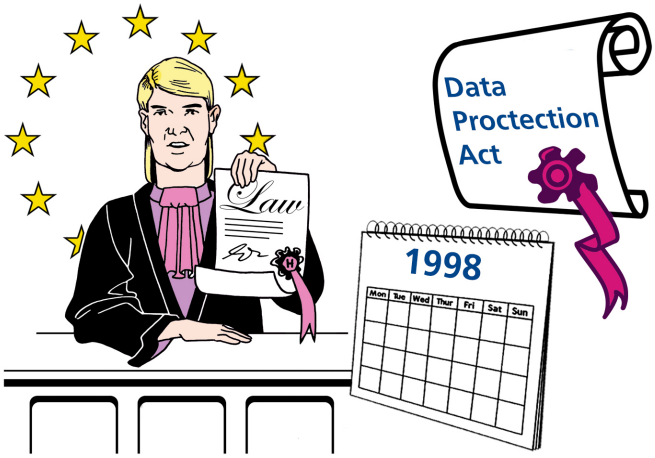
What you need to know about GDPR

For Staff and Volunteers

CHANGE

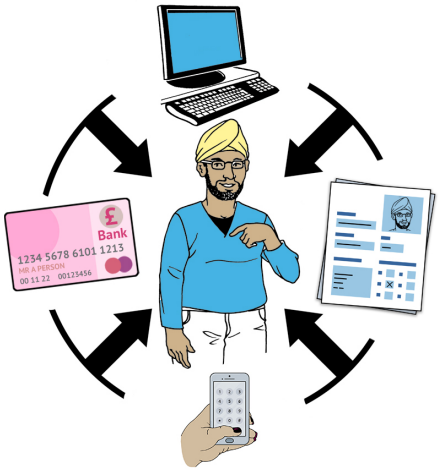


Easy Read



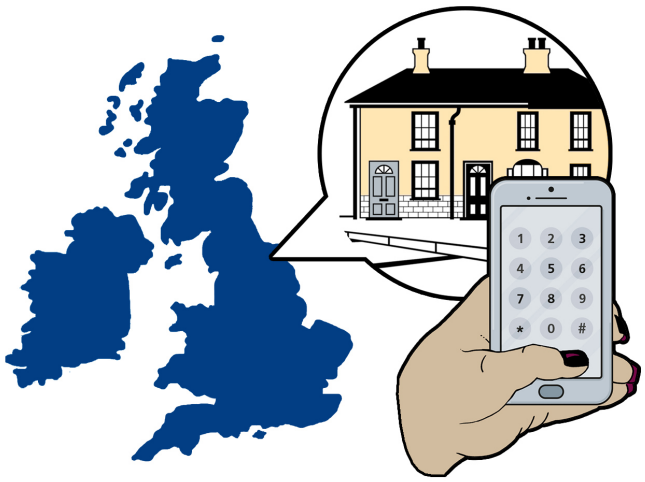
In 1998, a law was introduced in the EU about how your personal information needs to be protected. This law is called the Data Protection Act.

Personal information is any information about you that identifies you as an individual and is not meant for everyone to know.



This can include, but is not limited to:

- Your gender, date of birth and if you are gay, bisexual or straight.

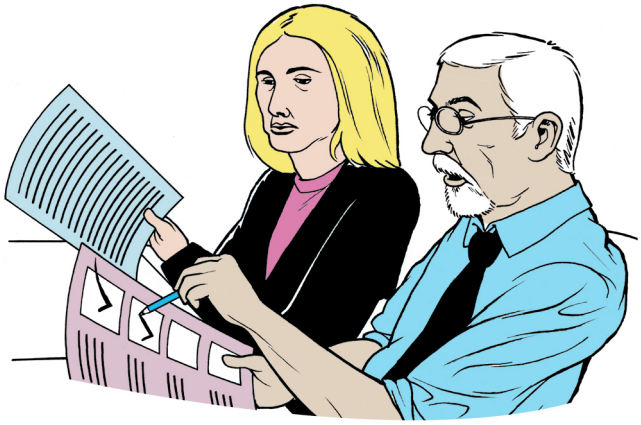


- Your address and phone numbers

- Information about your disabilities or health

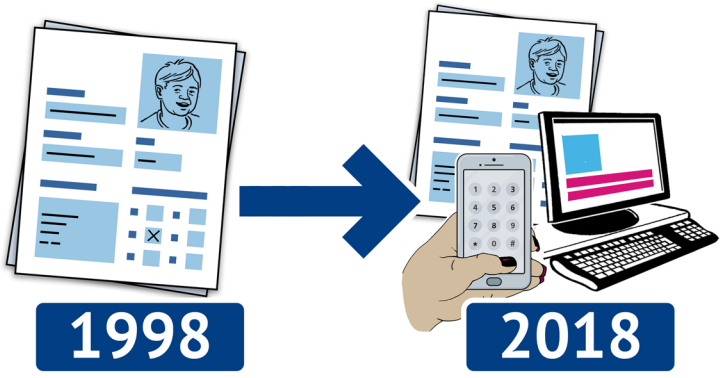
- Your bank details

- Information about your employment, like how much you get paid, or if you have ever ot into trouble at work



- Notes from your supervisions or appraisals

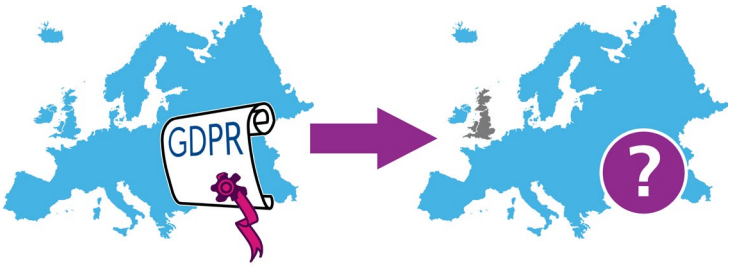
- Your personal opinions about someone



Since 1998, a lot has changed around how personal information is collected and used.

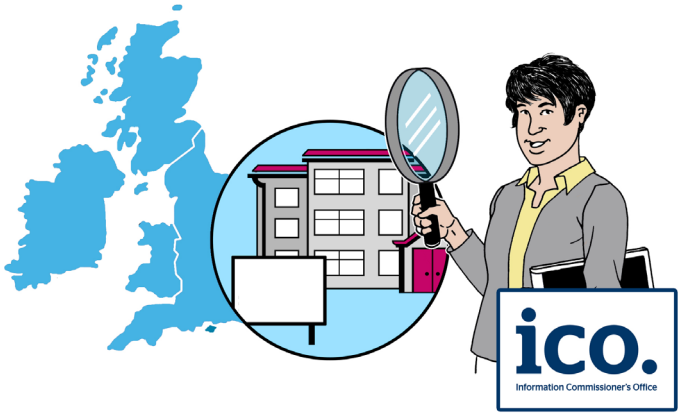
We give out our details more often, like when we buy things online, when we subscribe to newsletters, or when we apply for jobs and volunteering opportunities.

This is why there is a new law from the 25th of May 2018 that says how your personal information needs to be protected. This new law is called **The EU General Data Protection Regulation**, in short GDPR.



Because the UK is still in the EU, all organisations need to follow this law. After the UK leaves the EU, this law may stay the same or a new one will replace it. We do not know yet.

The Information Commissioner's Office, in short ICO, is a public organisation that reports directly to Parliament. This organisation makes sure that everybody who has to follow GDPR law does so.

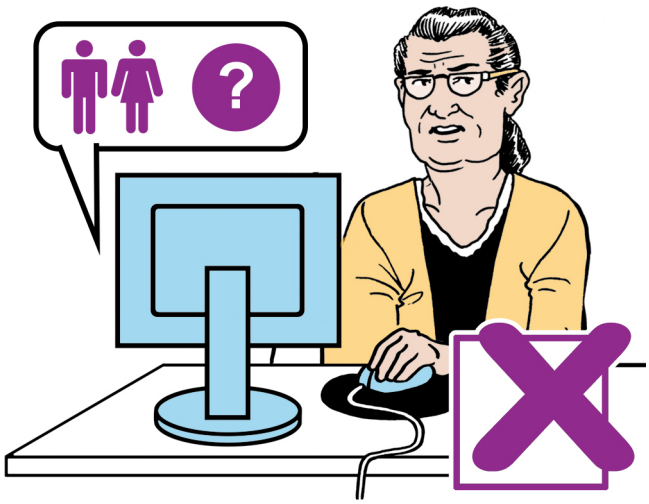


They can investigate organisations to see if they follow the GDPR law. They can also fine them if they do not.

About GDPR

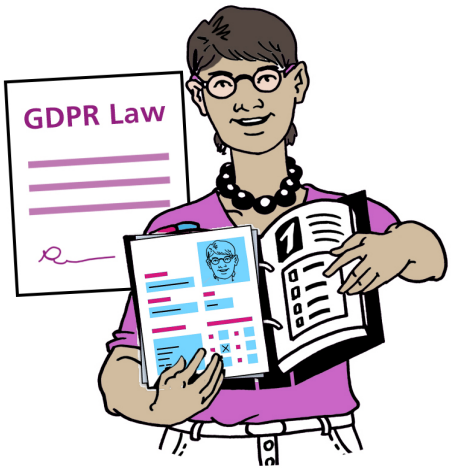
GDPR covers a few things:

- **Making sure data is collected responsibly.**
  This means that personal data must be collected in a fair and responsible way, which follows the law.

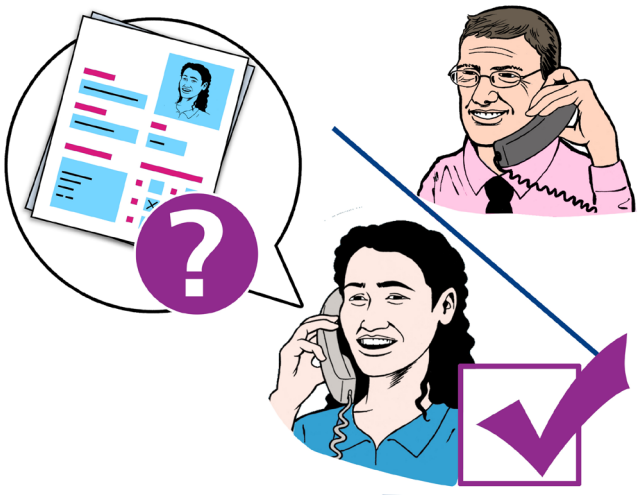


It also stops people and organisations from collecting more personal information than they actually need to. For example, you don't need to tell the online shop what your gender is when you buy a sofa.

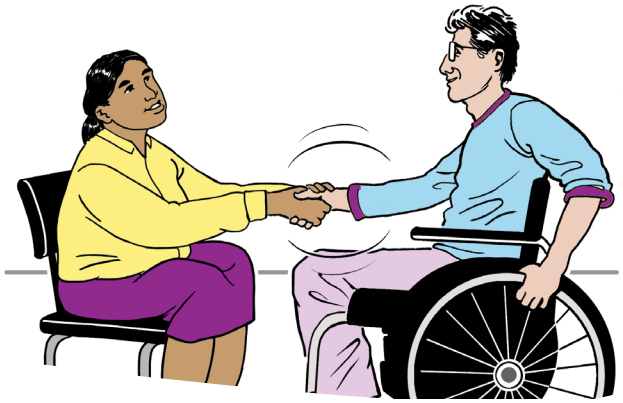
GDPR makes sure organisations and their employees understand that it is their responsibility to look after the personal information they hold.



- **Protecting rights**
  The new law outlines very specific rights for individuals. It also makes sure these rights are followed.



- **Making sure there is transparency**
  This means that individuals have the right to know who holds information about them, why they have it and how it will be used.



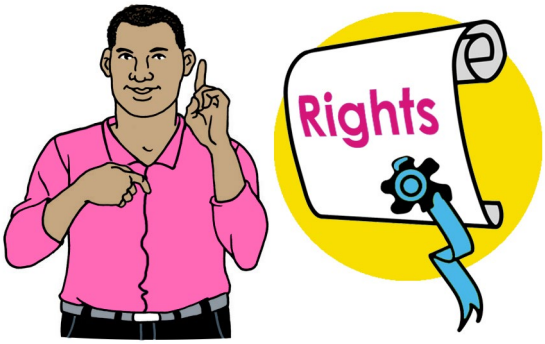
The aim is to build trust by being open, honest and transparent.

- **Preventing abuse**
  The law makes sure that information moves in a free, safe and secure way across Europe.

It also makes sure that everyone is treated equally and fairly.

The law also protects people from criminal activity and abuse of power.

Individual Rights



As an individual, you have a set of rights when it comes to protecting information about you. GDPR outlines these rights. They are:

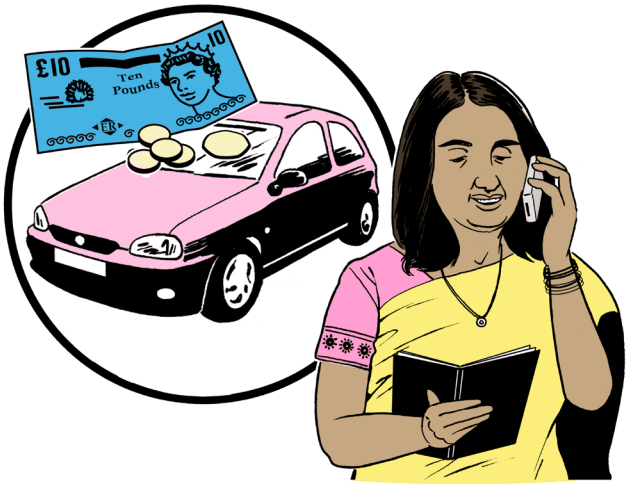
- Your right to be informed on how information about you will be used

- Your right to make changes to information about you that is incomplete or wrong

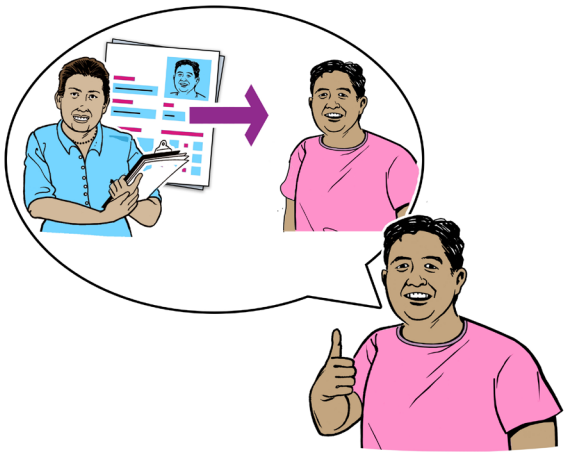
- Your right to stop an organisation from processing your data

Processing your data is when information about you is put on a system, looked at, analysed, used for reports or filed by an organisation

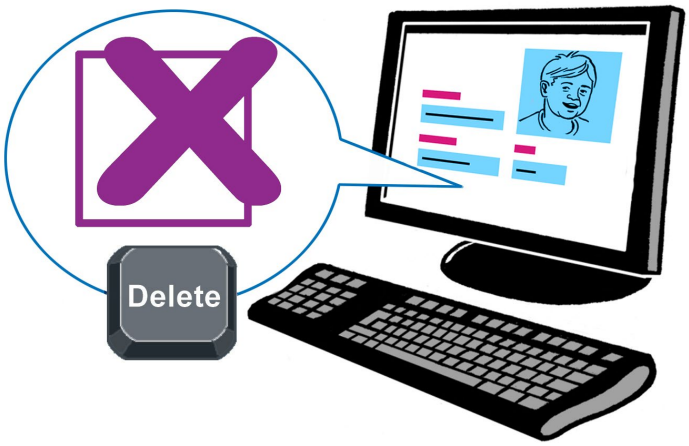
- Your right to say no to your information being processed or to direct marketing



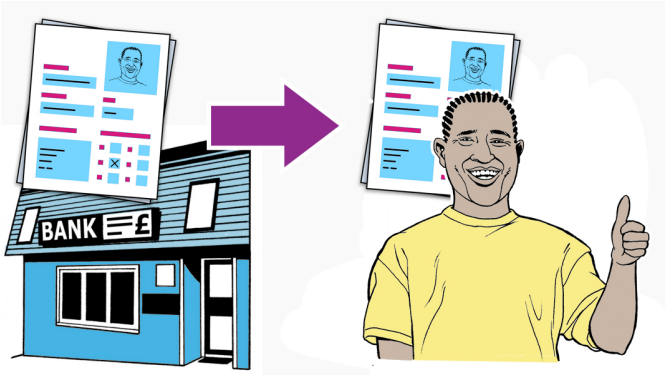
Direct marketing is when a company contacts you directly to sell or advertise their products or services.



- Your right to see a copy of the information others have on you.

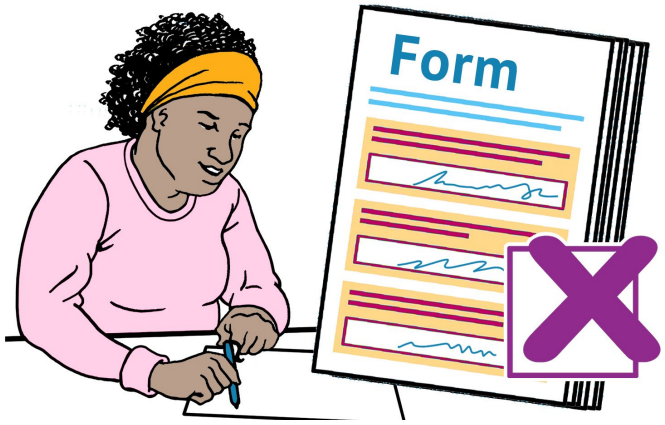


- Your right to ask for the information others have on you to be deleted.



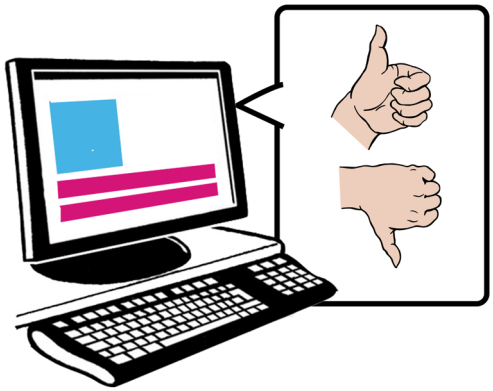
- Your right to ask an organisation for the information they have on you for you to have and use as you like.

As an example, when you fill in an application for a bank loan with one bank, if you want you can ask for a copy of that information to give to another bank when you apply for a loan there.

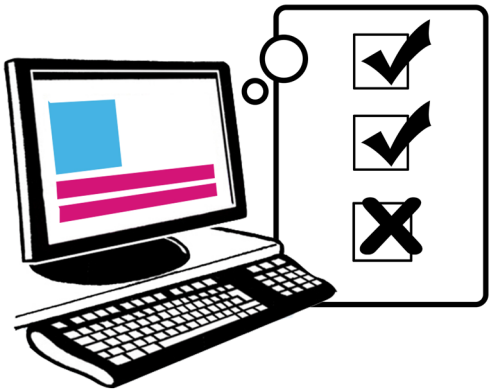


This means you do not have to fill in an application again from zero. This will save you time.

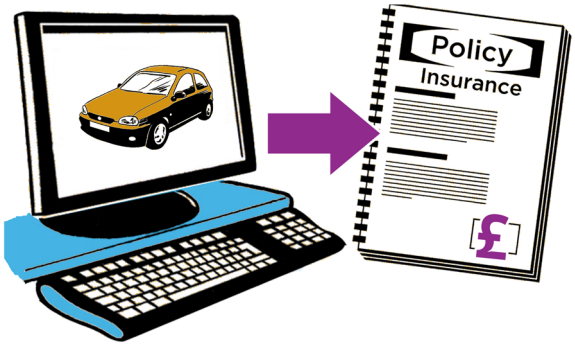
- Your right to have decisions about you made by a person



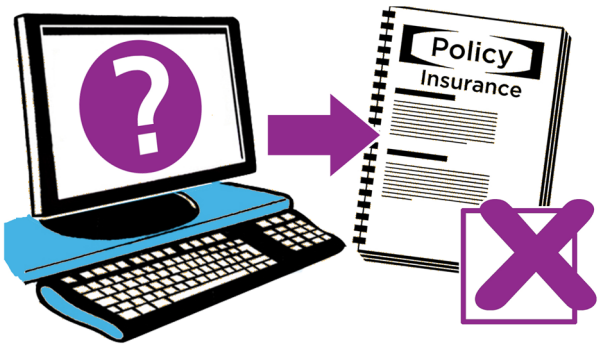
Some organisations use a system to make decisions. These systems are automated, like a machine.



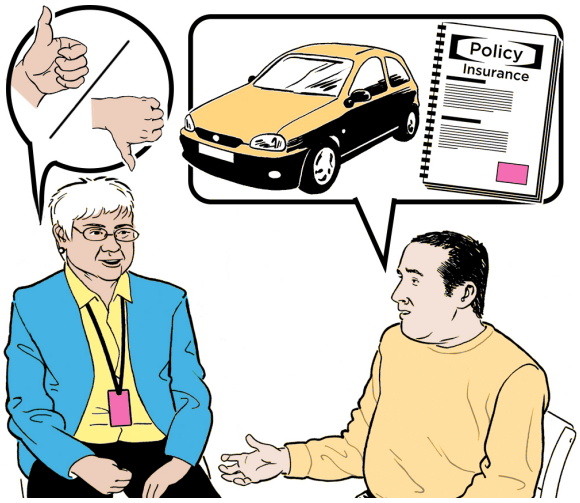
They will not look at everyone as an individual, but make decisions based on some very specific information.



For example, think of websites that compare car insurance. You will fill in information in a form, and then the system will give you a quote.



But the system will also use information available to it on people who have made a false claim in the past on their insurance. This information may be wrong or out of date. And because of this you may get a higher insurance quote or be refused a quote.



In a case like this, you can ask to have a real person look at your details and make a decision on the quote for your car insurance.

This means that you could discuss with them all the information they use in this decision, and this way find out if they have wrong information about you.

GDPR Roles

For GDPR to work, there are some organisations and people who have different roles in making sure the law is obeyed. They are:

- **Data subject**

  This is the name given to every person when talking about them in relation to their personal information. This is you!

- **Data Processor**

  These are people, organisations and companies who collect and use your personal information in any way. They can be an online shop or a clerk at the bank.

- **Data Controller**

  This is the person in any organisation who decides how and why personal information is processed.

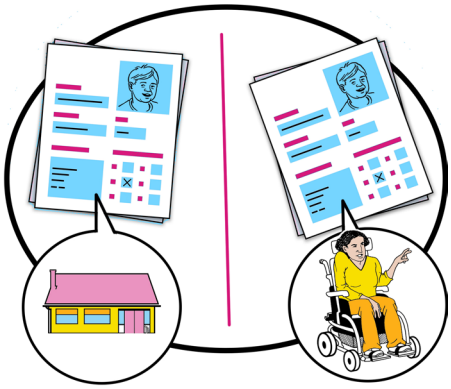
- **Data Officer**

  This is the person in any company who makes sure the law on data protection is followed.

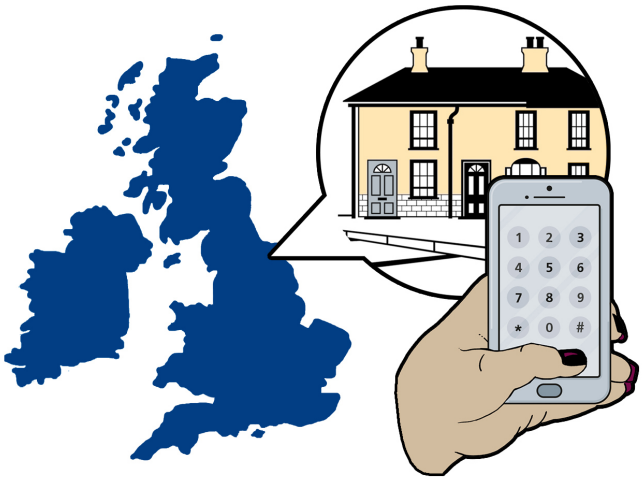
- **The Information Commissioner's Office**

- **The European Data Protection Board**

  This is an organisation that gives guidance to Data Controllers and Data Officers.



The new law splits data in two categories:

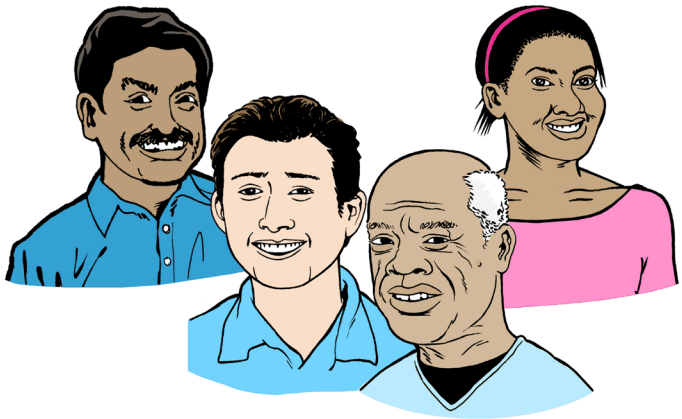


- **Personal Data**

  This is general information about you, like your address, phone number or date of birth.

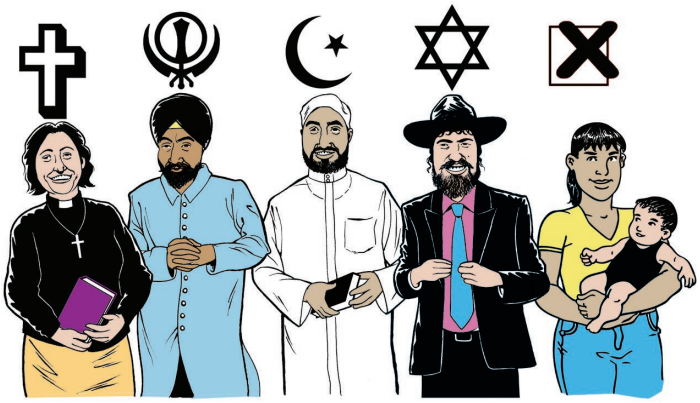
- **Special categories of personal data**

  This category refers to more sensitive information about you, like:

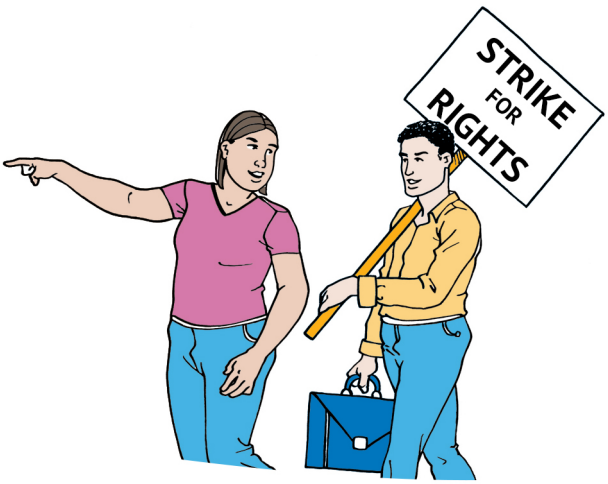


1. Your race or ethnic origin

2. Your opinion about politics and things related to politics

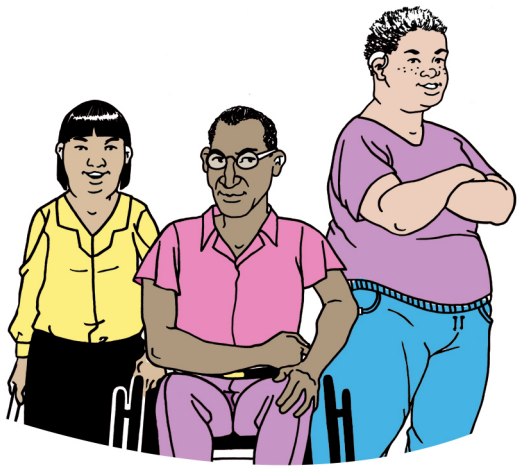


3. Your religion or beliefs



4. If you are a member of a trade union

5. Information about your sex life, like if you are gay or transgender



6. Special information about your genes and your body, like that in biometric documents

7. Information about your physical or mental conditions

The Six GDPR Principles

1. **Process information in a fair and legal way**

Any person or organisation should only collect the information they actually need.

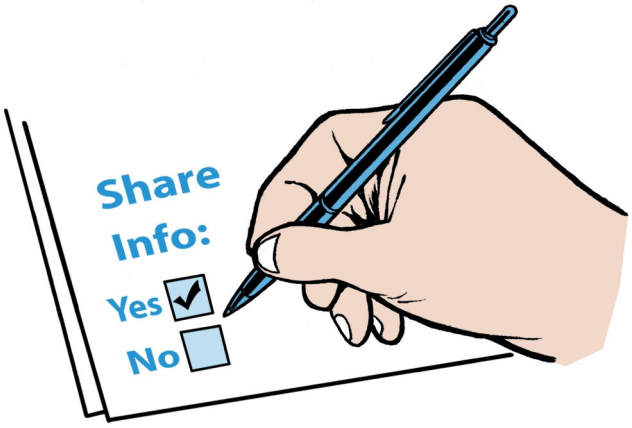
Information should not be used in a way that harms people.

The use of information needs to be transparent. This means that the way it is used must not be hidden, or used for reasons or in ways which are hidden.

It is also forbidden to do anything illegal with personal information.

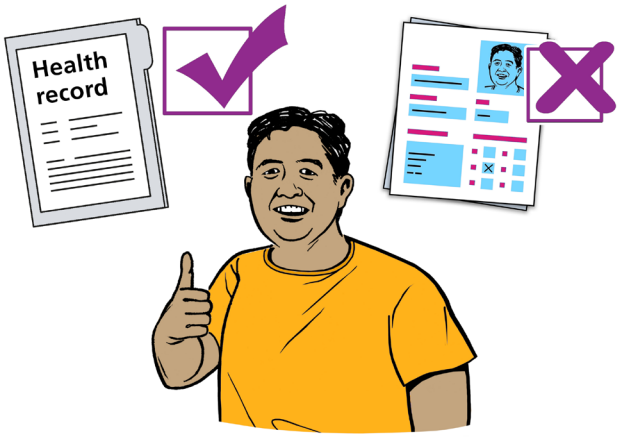
2. Use information only for the reason it was collected

When asking for personal information, any person or organisation needs to be very clear on why they are asking for it.



The law says a person needs to have the option to opt in to having their personal information collected.

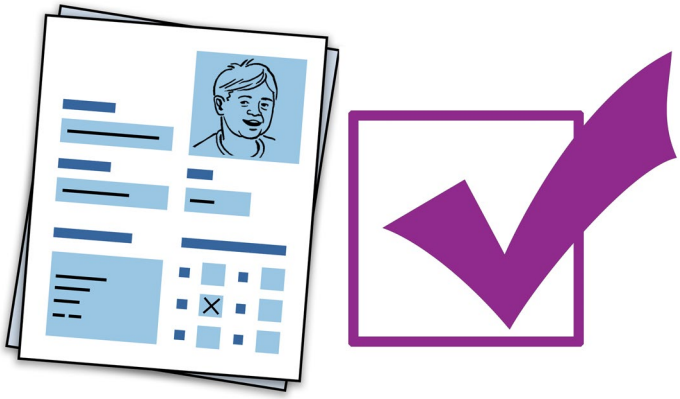
It is the responsibility and obligation of the person or organisation that collects this information to give you the option.



The same way, the person or organisation that collects such personal information needs to make sure you have an easy way of saying if you don't want your information to be used for anything else than the reason you gave it to them.

3. Only collect information that is relevant and needed

This means that only the information that is needed must be collected. Collecting more information than is needed for the purpose it is collected is illegal. Think of the example on buying a sofa online we gave before.



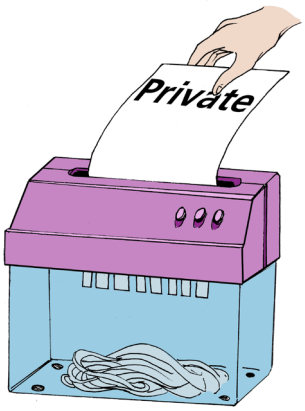
4. Collected information needs to be correct and up to date

Organisations and people who collect personal information need to make sure they take all the steps they need to make sure the information they collect and hold is correct.

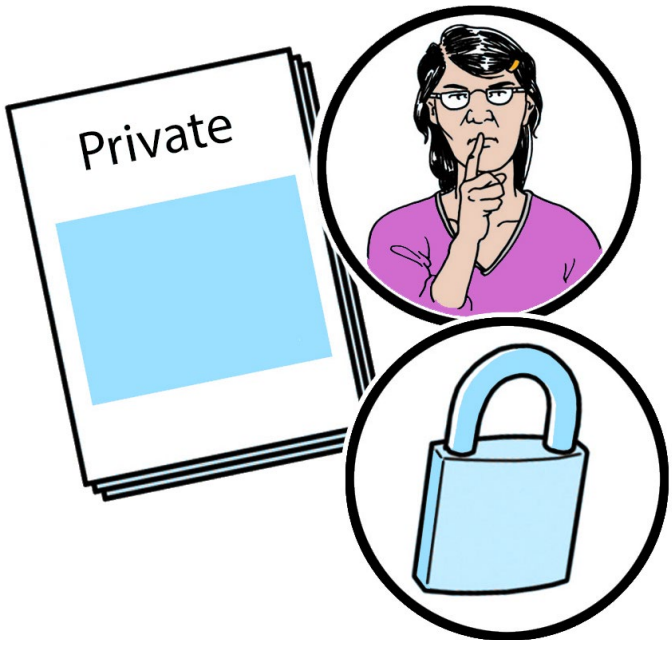
This also includes where they get their information. The source of it must be clear. You would not ask a child how much their parents spend each month on their energy bills, would you?

5. Not keeping information for longer than necessary

Organisations and people who process personal information need to look at how long they keep information for and what is the reason for which they keep it.



When the personal information they have is no longer useful or when it becomes out of date, they need to make sure that they delete or destroy it in a very secure way.



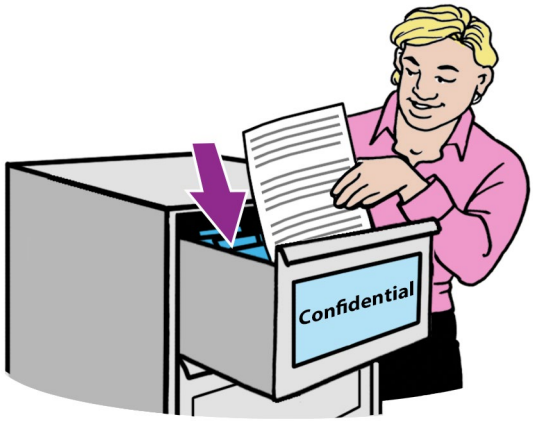
6. Process information securely

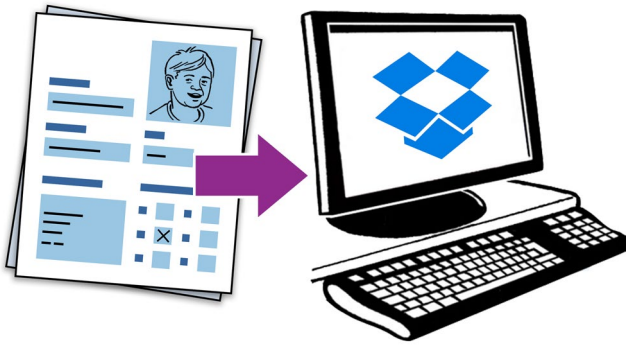
People and organisations who process data need to make sure they have the right security measures in place to make sure that nobody who isn't supposed to can access this information.

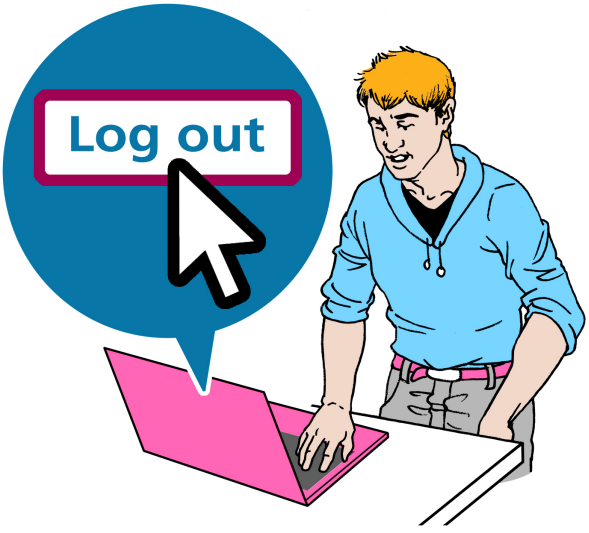
They need to be very clear about who is responsible for keeping information safe, and that they have the right policies that explain what everyone needs to do to keep information safe.

They also need to be ready to report it straight away if someone who isn't supposed to manages to access this personal information.

Think of everything you've learned about GDPR, about personal information and about your rights and responsibilities.



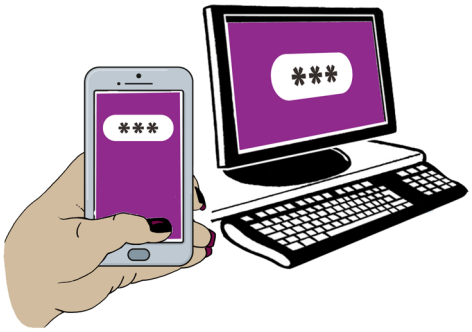




Now ask yourself:

- Do you have any paper files with personal information on them? Where do you keep them? Are they stored in a secure way?
- Do you ever upload personal information on external websites like Dropbox?
- Do you delete personal information after you no longer need it?
- Do you leave personal information visible on your screen when someone else can see it from behind you? Do you log out when you leave your desk for more than a minute or two?

- Do you need to take documents with personal information outside the office? Like when you are working from home. If you do, do you keep them safe?

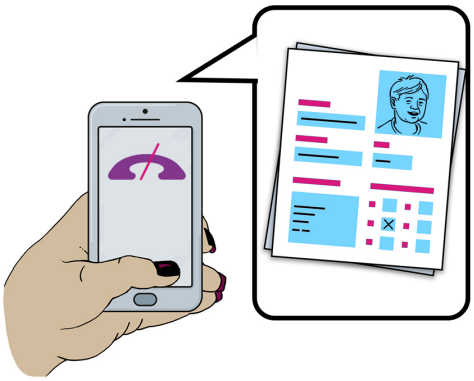


- Do you have a password on your computer, laptop, tablet and phone?

- Do you give the Wi-Fi password to anybody?

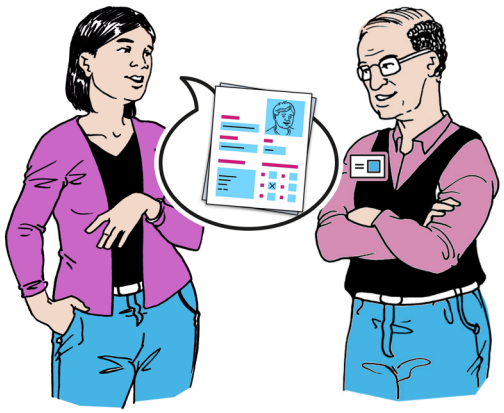
- When you receive or send confidential documents in the post, are these marked as “confidential”? Do you look after them properly?

- Do you make sure the person you are speaking to on the phone is truly who they say they are before you give them personal information?



- Do you ever leave confidential information on a voicemail?

- Do you ever discuss confidential information with someone while other people are around? What about in cafes or in open offices?



- Do you discuss confidential information only with the people who need to know it?

This easy read document has been produced by CHANGE
www.changepeople.org