GDPR

General Data Protection Regulations

WORKBOOK

Learning Log

Section of session	Key learning point

Action Plan

Action	Priority	When by?

Introduction

Think about the amount of personal information you share with other people. These may be people you know, or they may be complete strangers.

Do you use social media sites? If so, you are allowing other people to see a great deal of personal information about you?

Perhaps you shop online or use the internet for an array of other purposes. What about mobile devices such as telephones?

Even if you don't make much use of technology you still need to shop, bank, work, buy insurance and take part in many other activities. Think about the personal information that other people hold about you as a result.

Do you use a doctor, a dentist, an optician? These people may hold some very sensitive information about you, and they are not the only ones.

It is frightening to think that so much information is collected throughout our lives. This information is vulnerable to misuse if it is not properly protected.

We all have legal, moral and ethical responsibilities to keep other people's data secure and to ensure that it is not misused. The legal responsibilities are set out in the EU General Data Protection Regulations (GDPR) designed to protect us as individuals. It also has special rules for minors who are potentially more vulnerable than adults, particularly in online environments.

The organisation you work for has policies processes and procedures in place that are designed to meet the requirements of GDPR. It is vital that you follow these to ensure that the organisation and you personally are doing everything that is necessary to comply with the law.

What can go wrong? - Activity

Note examples of any situations where your personal data has been used for a purpose you have not agreed to or there has been some other problem with it. Alternatively, note examples of businesses or organisations that you know have failed to protect personal data properly.

Consider why these situations have gone wrong and what the actual or potential consequences are for the individuals affected.

In the News

You can find examples of prosecutions and enforcement action on the Information Commissioner's Office (ICO) website. Here are four of the cases reported by them.

Liverpool firm fined £70,000

The Lead Experts Limited were fined £70,000 for making 111.072 nuisance calls to private individuals. They were illegally responsible for making automated calls to people who had not agreed to them

The firm had bought contact details from another company who they paid to carry out the calls, which were about reducing energy bills.

Following the ICO's investigation, Companies House posted plans for The Lead Experts to be struck off and dissolved.

Reported on ICO website 13 October 2017

North London Council fined

Islington Council were fined £70,000 because personal information on its parking ticket system was not secure. Their system allows people to see CCTV images or videos of their alleged parking offences.

A design flaw meant that the personal data of nearly 89,000 individuals could be accessed by other people. This included some sensitive personal information such as medical records disclosed in appeals.

Sally Anne Poole, ICO Enforcement Manager, said:

"People have a right to expect their personal information is looked after. Islington Council broke the law when it failed to do that."

The council should have tested their system before it went live, and at regular intervals. From May 2018 the GDPR, requires a privacy impact assessment to be carried out when using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals.

Reported on ICO website 17 August 2017

Health worker fined

Whilst working for the Colchester Hospital University NHS Foundation Trust, Brioney Woolfe illegally accessed the medical records of 29 people without authority. These included members of her family, some colleagues and some strangers. She also shared some of this information with other people.

This was a breach of both patient confidentiality and data protection law.

She was fined £400 for obtaining personal data plus £650 for the offence of disclosing it to others. She was also ordered to pay a contribution of £600 towards prosecution costs, plus a victim surcharge of £65.

Reported on ICO website 17 August 2017

TalkTalk fined £100,000

The ICO fined TalkTalk Telecom Group PLC £100,000 because there was a risk that customers' data could falling into the hands of criminals

This came to light when TalkTalk started to get complaints from customers about scam calls. Scammers pretended they were providing support for technical problems and could quote customer addresses and TalkTalk account numbers.

The problem was a TalkTalk portal through which customer information could be accessed. One company with access was Wipro, a multinational IT services company in India that worked on behalf of TalkTalk.

Forty Wipro employees had access to the data of up to 50,000 TalkTalk customers and could log in to the portal from any internet-enabled device.

The ICO found this level of access was unjustifiable and put the data at risk.

The ICO investigation did not find direct evidence of a link between the compromised information and the complaints about scam calls. Nevertheless, they fined TalkTalk for having inadequate control measures.

Reported on ICO website 17 August 2017

Purpose and application

The GDPR develops existing data protection law which aims to strike the right balance between the rights of individuals and the interests of those with legitimate reasons for using personal information.

It also modernises existing Data Protection law because the world has changed a lot in the last 30 years. For example, technology has advanced at a pace and the way in which we use it has changed dramatically.

It is now commonplace to shop online and to use various different types of social media. The way in which organisations use our information has also changed.

One of the main aims of GDPR is to provide standardised data protection laws across the EU. The intention is to make it easier for individuals to understand how their data is being used and to be able to raise complaints if necessary.

The UK will still be a part of the EU when the regulations come into force, so they will definitely apply. However, there is some uncertainty over what will happen when the UK finally leaves. There seem to be two main scenarios.

1. If the UK joins the European Economic Area then it will continue to be subject to GDPR.

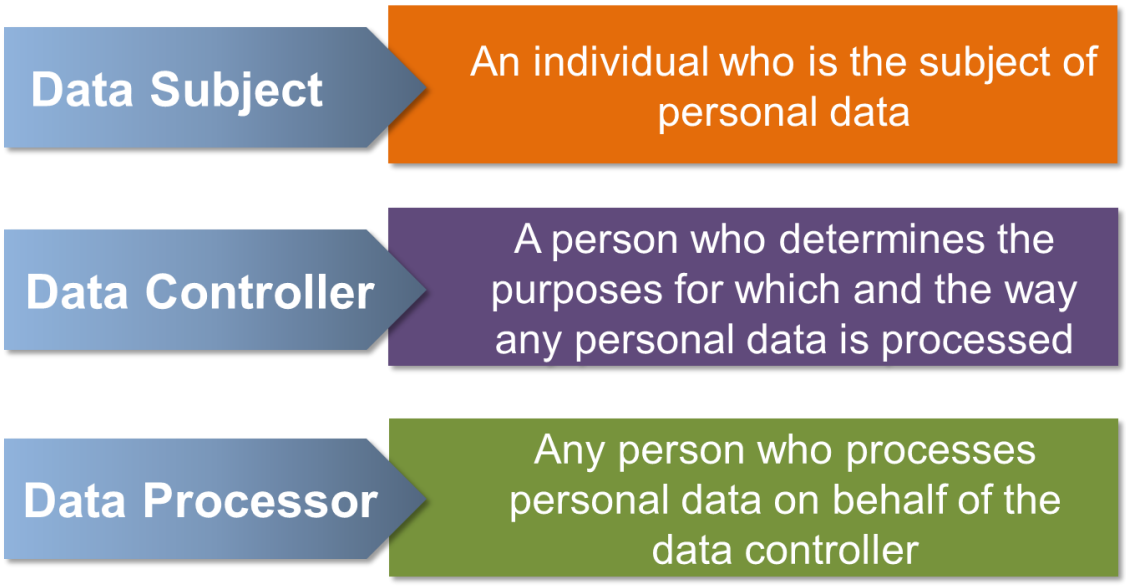
2. If it does not leave, the GDPR will not apply. However, the UK will need to show that it has adequate data protection provisions in place if it is to trade in Europe or to cover organisations that hold the personal data of EU citizens. This means that we can expect the UK government to pass its own law giving equivalent protection.

Either way, there really is no choice. Any business or organisation based or operating in the UK or any EU state must ensure that it is GDPR compliant.

Incidentally, this is not just about complying with EU law. It will also be necessary to show that data protection in the UK is of a standard that is acceptable to other global trading partners.

GDPR helps to minimise the threats posed to us as individuals as a result of all of the information held about us.

Before moving on, it will help to understand three terms that will be referred to throughout this workbook.



Obligations and responsibilities under the GDPR apply to 'controllers' and 'processors'.

The GDPR places specific legal obligations on processors. For example, they must keep and maintain proper records of their personal data and processing activities.

Controllers are also subject to specific requirements. For example, they must be able to demonstrate that they are complying with the regulations.

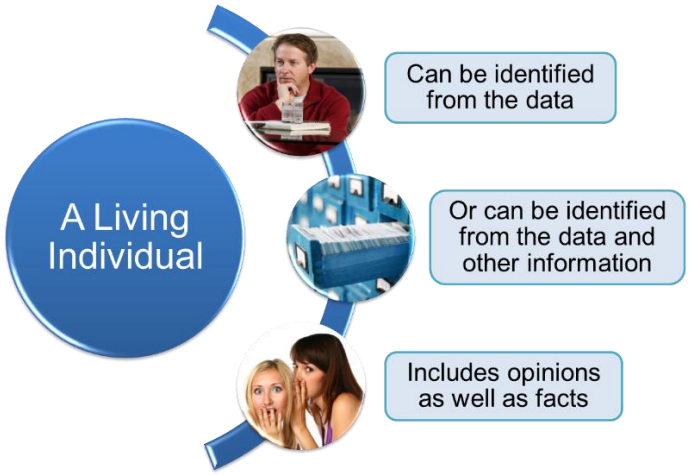
Types of Personal Data

The GDPR applies to personal data. In simple terms if it is possible to identify the individual it relates to then it falls under the GDRR.

It is also important to understand that the GDPR is not confined to data stored in computer records.

These are also two types of data protected by the GDPR. These are:

- Personal data
  and
- Special categories of personal data



Personal data relates to a living individual who can be identified from that data. It is covered by the GDPR if it relates to that individual's private, professional or public life.

According to the European Commission it can be anything from a name, a photograph, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address. It covers any factor that could be used to identify an individual.

It is also personal data if the individual can be identified from it when it is combined with other information.

It does not only cover facts about the person. It includes opinions, decisions or proposed decisions about the individual or anybody connected to them. For example, if a person is declined credit based on information about their spouse.

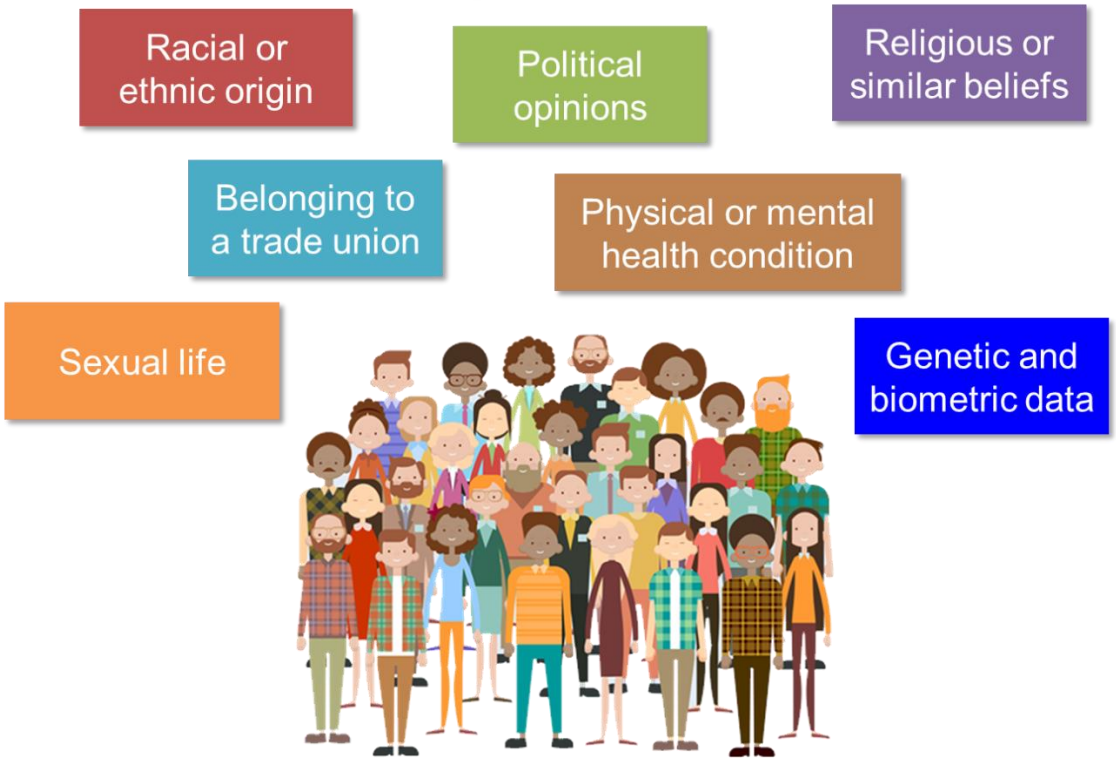
Special Categories of Personal Data

This used to be known as sensitive personal data and is similar to it, with some changes. Data processors and controllers must be particularly careful with this type of information.

Although personal data relating to crimes, alleged crimes or criminal proceedings do not fall within the special categories they are subject to similar safeguards.

The special categories are:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Whether or not they belong to a trade union
- Physical or mental health or condition
- Sexual life
- Genetic and biometric data where it is processed to uniquely identify an individual



Is it a Special Category? - Exercise

Can you identify the difference between personal data and special categories of personal data?

Have a look as the following grid and decide if the information would be classed as personal data or as a special category of personal data. Just tick the appropriate box for each of them.

	Personal	Special
Name		
Address		
Trade union membership		
Customer orders		
Religious belief		

Criminal convictions		
Criminal charges		
Political opinions		
Bank account		
Telephone Number		
E-mail address		
Racial or ethnic origin		
Sexual life		
Physical health		
Mental health		
Disabilities		
Genetic and biometric data		

Address book – Exercise

We all keep records about our families, friends and other people at home. This is usually for contact details but may also include other information such as birthdays and anniversaries.

This may be in the form of a paper address book or perhaps you store this information on a personal computer, mobile phone or other device.

You may also be storing this information online.

To what extent, if at all, do you think that this information may be regulated by the GDPR.

GDPR Principles

If you are subject to the GDPR you must comply with its principles. These are set out in the regulation itself and stipulate that all personal data must be:

Fair and lawful processing	Processing of data must be lawful and fair and performed in a transparent manner in relation to individuals.
Specified lawful purposes	Personal data must be collected for specified, explicit and legitimate purposes and not 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 incompatible with the initial purposes.

Adequate and relevant	Personal data must be adequate, relevant and limited to what is necessary for fair and lawful processing.
Accurate and current	The data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
Kept no longer than necessary	Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for fair and lawful processing. It may be stored for longer periods if it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. However, your firm must implement appropriate security measures to safeguard the rights and freedoms of individuals.
Appropriate security	The data must be processed in a manner that ensures appropriate security using appropriate technical or organisational measures. This includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage.
Proving compliance	Controllers of personal data are responsible for compliance with these principles. They must also be able to demonstrate compliance.

Criminal convictions do not fall within the definition of 'special category of personal data', and are dealt with separately.

However, for most practical purposes they are protected in a similar way. This means that you must treat them with the same level of care as you would a 'special category'.

International

Organisations that transfer data outside of the EU are required to be aware of the potential risks that this involves.

They are obliged to ensure that the data is safe, if they do transfer it in this way.

Non-EU organisations may need to appoint representatives in the EU if they are handling the personal data of EU residents.

In both cases, the obligation is to ensure compliance with the GDPR principles.

Processing Personal Data

To process data lawfully it is necessary to be able to have a legal basis for doing this. This means that it must be processed in accordance with at least one of the conditions set out in the GDPR. You can find a summary of the main conditions below.

Consent of the individual	This is very simple. If the person agrees to it, then their data can be processed. The consent must be explicit which means that it cannot be assumed or given by means of pre-ticked boxes on application forms.
Performance	This applies where processing is necessary for the performance

of the contract	of a contract with the data subject or to take steps to enter into a contract with the data subject. For example, it would be necessary to process the customer's address to deliver goods ordered by a customer.
Legal Obligation	Some processing is required by law. A good example of this is employment law which require certain information to be collected during the recruitment process.
Vital interests	Sometimes it is necessary to process data to protect the vital interests of a data subject or another person. For example, a doctor may need to access a patient's medical records.
Public interest	Processing is sometimes necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. An example might be the use of certain databases to help combat financial crime.
Necessary to pursue legitimate interests	Data may be processed when it is necessary for the purposes of legitimate interests pursued by the controller or a third party. However, this may be over ridden by the interests, rights or freedoms of the data subject.

Special categories of personal data were formerly known as sensitive personal data.

Special care is required for this type of data. In addition to the above there are other situations where this data may be processed or stored. Some of the main conditions are outlined on the next page.

Additional conditions for processing special categories of personal data. One of these or one of the conditions shown in the previous page must apply, to enable the data to be processed or stored. Alternatively, it may be shown that it is necessary to process the data for any of the following reasons.

Substantial public interest	This applies if processing is necessary for reasons of substantial public interest based on EU or Member State law. This must be proportionate to those interests and the data must also be subject to appropriate safeguards.

Health	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services based on Union or Member State law or a contract with a health professional.
Public Health	This applies where processing is necessary for reasons of public interest around public health. This includes protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
Archiving and research	Processing is allowed where it is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

It is important to emphasise the importance of obtaining the data subject's consent to process his or her personal data. If this is obtained, then this normally enables us to process the data.

When obtaining an individual's permission to process his or her data, this must be a positive act of consent. It will no longer be possible to assume that silence or inactivity amounts to consent. Clear and explicit consent to process personal data must be obtained.

If the individual is under the age of 16 then consent must be obtained from a person with parental responsibility for the child in some cases.

Myths and Realities – Exercise

Consider these statements. Which do you think are correct and which are false?

	True	False

1.	The GDPR stops parents from taking photographs in schools.		
2.	The GDPR means a company is never allowed to give a customer details to a third party.		
3.	The GDPR stops parents finding out their children's exam results.		
4.	The GDPR prevents priests from naming sick parishioners during prayers.		
5.	The GDPR prevents the release of offenders' details to victims.		
6.	The GDPR prevents organisations from processing or storing the personal data of children.		

Who can you give information to? – Exercise

Look at the following list and consider whether we can disclose the data.

	Yes	No	Maybe
1. The customer making an enquiry about his account.			
2. A relative of your customer making an enquiry about the account.			
3. A bank wanting details of one of our employee's earnings, so they can process a mortgage application.			
4. You get a call from the citizen's advice bureau making a complaint on behalf of your customer.			

Our Eight Rights

Under the GDPR individuals have eight data protection rights. They are:

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

1. Right to be informed

This right is about transparency requires us to tell individuals that we are processing their data and the reason(s) for this. This is known as 'fair processing information' and will normally be found in a privacy notice.

According to the Information Commissioners Office (ICO), the information we supply must be concise, transparent, intelligible and easily accessible. It must be written in clear and plain language, particularly if addressed to a child. It must also be free of charge.

The information we must provide depends on how we obtained the data.

Information obtained direct from the data subject

Fair processing information must be provided when the information is being collected. According to the ICO, this should include relevant information from this list:

- Identity and contact details of the controller, or representative, and data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Any recipient or categories of recipients of the personal data
- Details of transfers to a country outside of the EU and the safeguards in place
- Retention period or criteria used to determine the retention period of the data
- The existence of each of data subject's right
- The right to withdraw consent at any time, where relevant
- Whether providing the personal data is a statutory or contractual requirement or obligation, and the possible consequences of failing to provide it
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Information that is not obtained direct from the data subject

Fair processing information must be provided within a reasonable period of obtaining the data (within one month at the latest).

If the data is used to communicate with the individual, then it must be provided during the first communication.

If it is being passed to a third party the fair processing information must be given before it is disclosed to the third party,

2. Right of access

Individuals have the right to access the following information:

- confirmation that their data is being processed;
- access to their personal data;
- any other supplementary information

We have this right so that we know about the processing and so that we can check whether our data is being processed lawfully.

We must normally provide this information free of charge.

However, we can charge a reasonable fee when the request 'is manifestly unfounded or excessive, particularly if it is repetitive'. It is also possible to charge a fee if more copies are requested,

Any fee must be based on the administrative cost of providing the information.

We must provide the information without delay and within a month, at the latest.
If the request is complex or numerous then it may be possible to extend this period by a further two months. However, we must tell the individual the reason why this delay is necessary.

Unless you have explicit authority to deal with subject access requests you should always refer them to the person identified in your firm's procedures. This is likely to be your manager.

3. Right of rectification

If personal data is inaccurate or incomplete individuals have the right to have this corrected.

If we have disclosed any of this data to any third parties, we must tell them that it has been rectified where this is possible.

We must also tell the affected individual which parties have received the inaccurate or incomplete information from us.

We must deal with rectification within one month. This can be extended by two months for complex requests.

4. Right of erasure

This is also known as 'the right to be forgotten'. Individuals may ask for their personal date to be removed where there is no good reason to continue processing it.

This right only exists in specific circumstances:

- the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- the individual withdraws consent.
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed
- the personal data has to be erased in order to comply with a legal obligation.
- the personal data is processed in relation to the offer of information society services to a child.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation
- for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
- or the exercise or defence of legal claims.

If we have passed the data to any third parties, we must inform them of the erasure unless this is impossible or involves disproportionate effort.

If the data was made pubic online then other organisations who process it must also be informed and must erase the data or any copies or links that point to it.

Children

There is extra protection for children, especially in the case of online data.

We must pay particular attention when a child withdraws their consent to process personal data and requests erasure.

This is particularly important on social networking and internet forums, as children may not fully understand the risks involved.

5. Right to restrict processing

This is an individual's right to 'block' or suppress processing of their data. This applies in the following circumstances:

- If an individual contests the accuracy of personal data, you should restrict processing until you have verified its accuracy
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful but the individual is opposed to the data being erased and asks for it to be restricted instead
- We no longer need the data but the individual needs it to make or defend a legal claim

If a restriction is in place we are allowed to store the data but may not process it.

We can keep the minimum amount of information necessary to ensure that the restriction is respected in future.

If we have disclosed the data to any third parties, we must tell them about the situation unless this is impossible or involves disproportionate effort.

We must also inform individuals when you decide to lift a restriction on processing.

6. Right to data portability

This allows individuals to obtain and reuse their personal data for their own purposes across different services.

This right only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract;
- and when processing is carried out by automated means.

We must provide the personal data free of charge and in a structured, commonly used and machine-readable form.

If the individual asks us to transmit their data direct to another organisation we must do this if it is technically feasible.

If the data is about more than one person we must consider whether the rights of any other individual is compromised.

We must respond without undue delay, and within one month.

This can be extended by two months where the request is complex, or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

7. Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling);
- and processing for purposes of scientific/historical research and statistics.

Legitimate interests

If we are processing personal data to perform a legal task or for our organisation's legitimate interest's individuals may only object on "grounds relating to his or her particular situation".

In those circumstances, we must stop processing that data unless:

- we 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.

Direct marketing

We must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse to do this.

If we receive an objection to processing personal data for direct marketing, we must deal with it no matter when it is made.

We must also do this free of charge.

If we are processing personal data to conduct research necessary to perform a task in the public interest, we do not have to comply with an objection.

8. Rights related to automated decision making and profiling

Automated decision making

Individuals are protected against the potential risk of being harmed by decisions made without human intervention.

We have the right to ask not to be subject to a decision when:

- it is based on automated processing;
- and it produces a legal effect or a similarly significant effect on us.

In these cases, the organisation must make sure that individuals may:

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

This right does not apply if the decision is:

- necessary for entering or performance of a contract with the individual;
- authorised by law;
- or based on explicit consent from the individual

Automated decision must not concern a child; or be based on the processing of special categories of data unless:

- it is with the explicit consent of the individual;
- or the processing is necessary for reasons of substantial public interest based on EU / Member State law.

This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Profiling

GDPR definition of profiling:

'…any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability; behaviour;
- location;
- or movements...'

If we use personal data for processing we are required to have appropriate safeguards, and this includes

- Ensuring that processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected 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 prevents discriminatory effects.

Refusal to comply

In all cases, if we refuse to comply with a request from an individual to exercise their rights, we must explain why we are doing this.

We must also inform the individual of the right to complain to the ICO or to seek a legal remedy through the courts.

Source: Information Commissioner's Office

Keeping Data Secure

Identifying the caller

There is a particular problem when dealing with people over the telephone. How can you be certain that the person on the other end of the phone is who they say they are?

The onus is on you to check their identity. Many organisations ask three security questions. Here are some examples. Of course, you must make sure that you ask the security questions you have been trained to ask in your own organisation.

Incidentally, we may be concentrating on telephone calls here, but similar principles apply to face to face conversations if you do not know the other person.

Here are some examples of security questions that are used in different businesses. However, you must use the questions you have been trained to ask in your own firm.

1st Question	2nd Question	3rd Question
• Account number • Reference number • Contract number • Phone number	• Name • Full name	• Password • Full address • First line of address • Post code • Date of birth • Payment method • Last payment made • E-mail address

Computer security

Data that is stored electronically on computers, computer systems or other electronic devices is potentially vulnerable.

This means that must take steps to keep it secure. Part of this is about ensuring that employees only have access to data that the need for their jobs. The use of menus, user profiles and passwords are important here.

It is vital that you use strong passwords and change them regularly. As well as following the tips shown on the screen below, you must also comply with your organisation's password policies, processes and procedures.

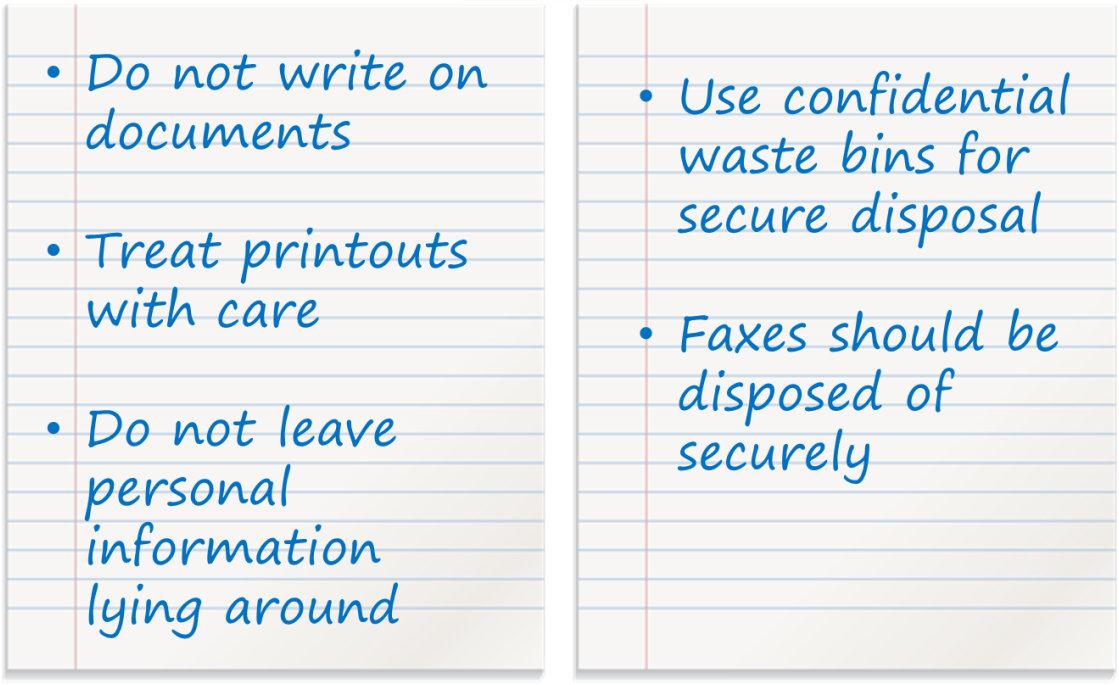
- Keep passwords secret
- Use strong passwords
- Do not allow others to use your computer identity
- Switch off or lock your screen when you are not there
- Only use data for the purposes of your job

Paper Records

It is just as important to protect personal data that is on paper. This applies just as much to your own rough notes as it does to formal paper records.

Unless it is a necessary part of your job you should avoid writing or printing personal data, especially if it is a special category.

If you do have to write or print it, you must keep it secure from prying eyes and dispose of it securely. Once again, be sure to follow your firm's policies, processes and procedures.



Making Notes

Remember that your own notes may form a part of an individual's personal data, whether you write them in a hand written or electronic format.

This means that you must make them with care. It is also worth bearing in mind that individual's may get to see your notes if they ask for access to their data.

Have a look at the information on the notice board below. There are some useful tips here.

Yet again, be sure to follow your firm's relevant policies, processes and procedures.

Do’s and Don’ts

Data protection is at least partly about ensuring that we take necessary action to protect personal data. It is also about avoiding actions that place that data at greater risk than is necessary.

Look at our list of do’s and don’ts and give them some thought.

Which of these apply to your job role?

Are there other do's and don'ts that you should be adding to the lists? If so, add them to the bottom of each list.

Do	Don't
• Carry out identify checks before discussing personal information • Only use personal data to do your job – never for any other purpose • Tell people what their data is being used for • Follow the organisation's security procedures • Use strong passwords and change them often • Dispose of information securely when it is no longer needed • If you are a manager, make sure your staff are trained	• Leave information lying around unattended • Forget physical security such as locking away paperwork overnight • Forget to lock your computer screen when it is unattended • Record anything that is unfair or untrue • Process personal data unless you are sure that the data subject has consented to it • Pass personal pass personal data to people who are not authorised to have it • Forget to check that information you gather is correct

Scenarios Activity

Scenario One

Mrs Wilson made a complaint about a faulty mobile phone. Her suppliers agreed to replace it. Unfortunately, she recently changed her address but the suppliers sent the replacement phone to her old address by mistake.

A man has now telephones explaining that Mrs Wilson has moved and that he now lives at her old address. He knows that she lives nearby but does not know her new address. However, he does know that Mrs Wilson moved to an address nearby. In an attempt to be helpful, the man suggests to the person dealing with the call that she should tell him Mrs Wilson's new address. He will then take the replacement phone to her.

The person who is handling this call has no doubt that the man is genuinely trying to be helpful and does not suspect any ulterior motive on his part.

What do you think she should do, and why?

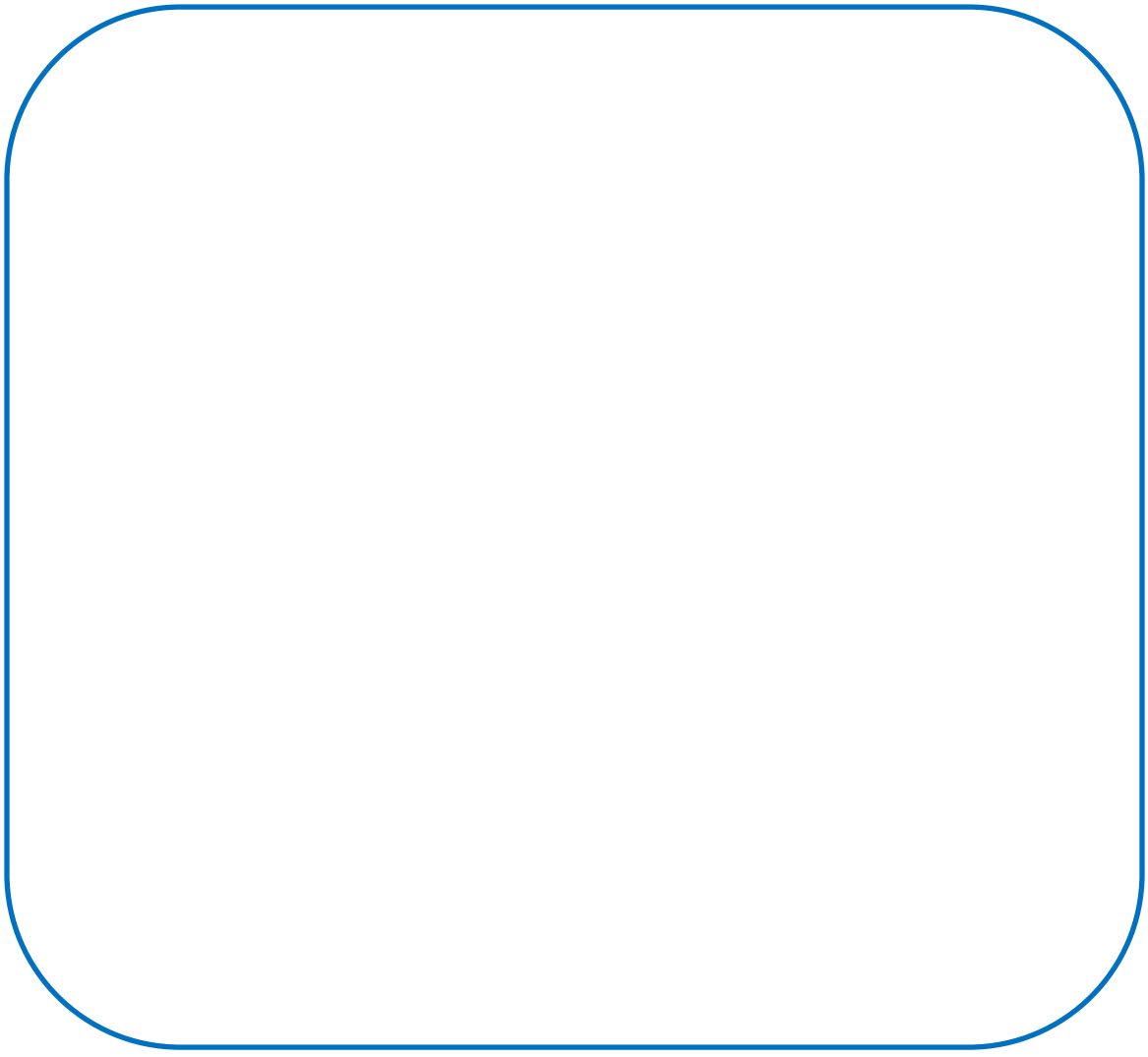
Scenario Two

Sarah is a very good friend who works for a rival company. She is responsible for recruitment, and explains that an employee of the company you work for has applied to her for a job. You know the job applicant well.

Sarah says that she is very keen to recruit this person but is aware that he has a medical condition. She asks you these questions:

- What do you know about this condition?
- Do you know whether it affects his ability to do his job?

You want to help Sarah but are not sure whether you can. What should you do?



Scenario Three

Paul had a motor accident when he blacked out whilst driving the car. Investigations by his insurance company revealed that his black out was caused by a previously undetected medical condition.

Nobody else was involved in the accident. When Paul blacked out he lost control of his car and collided with a tree at the side of the road. Paul and a passenger in his car sustained only slight injuries. His car was also damaged.

After some thought, Paul has withdrawn his claim and has paid for the cost of repairing the car out of his own pocket. His insurance company have also cancelled his insurance policy because of his medical condition.

He has asked the insurance company to remove all details of his illness from their records and has argued that these details are no longer necessary as he did not go ahead with his claim and his insurance has also been cancelled..

How do you think his insurance company should deal with this request?

Data Protection - Exercise

Here are ten statements about data protection. Look at each of these in turn and tick whether you think they are true or false.

		True	False
1.	The GDPR applies only to data held in or via computer systems.		
2.	A friend writes to you asking whether your firm has any job vacancies. You take the letter to the Human Resources department. The letter is subject to the GDPR.		
3.	You can only process personal data with the consent of the data subject.		
4.	It is permissible for you to discuss a customer's personal with his spouse.		
5.	Under no circumstances can you disclose personal data to another party without the consent of the data subject.		
6.	We must take extra care with special categories of personal data.		
7.	Financial information we have about a customer is a 'special category of personal data'.		
8.	If a data subject requests in writing that we provide all the personal data we hold about her, we must supply it. We can charge a small fee for this.		
9.	You are photocopying some customer details and accidentally produce too many copies. It is OK to take the surplus photocopies home to use it as scrap paper.		
10.	A 10-year-old child is registering a new computer game online and is being invited to sign up to the manufacturers social media site, Under the GDPR they must obtain authorisation from a person with parental responsibility for		

the child.		