Keeping organisational data secure

Version: 1.0

Effini

Data Education in Schools

Skills Development Scotland

Learning intentions

We will be looking at how organisations keep data secure, specifically,

- What happens if **organisations don’t keep data secure**
- What is **GDPR**
- What are your **data rights under the law**
- How encryption and backups **keep data safe**

Background

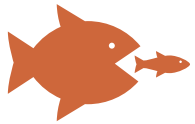
When you share your data with a company or organisation, you trust that they will keep it safe. Unfortunately this doesn't always happen.

In this lesson will look at times when **companies have not kept data secure**; and what **laws and tools** are in place to **protect the data** an organisation holds.

What could happen if data isn’t kept secure…

Customers could lose confidence in the company and stop doing business with them

Companies could be fined by organisations that oversee data protection



The competitors of an organisation could see their private information, which could give the competitor an advantage

Definition

Data breach

An incident that has affected the security of personal data

Next we will watch a **video on some of the worst data breaches**.

https://www.youtube.com/watch?v=0f-uFn-5hck

Top 5 data breaches

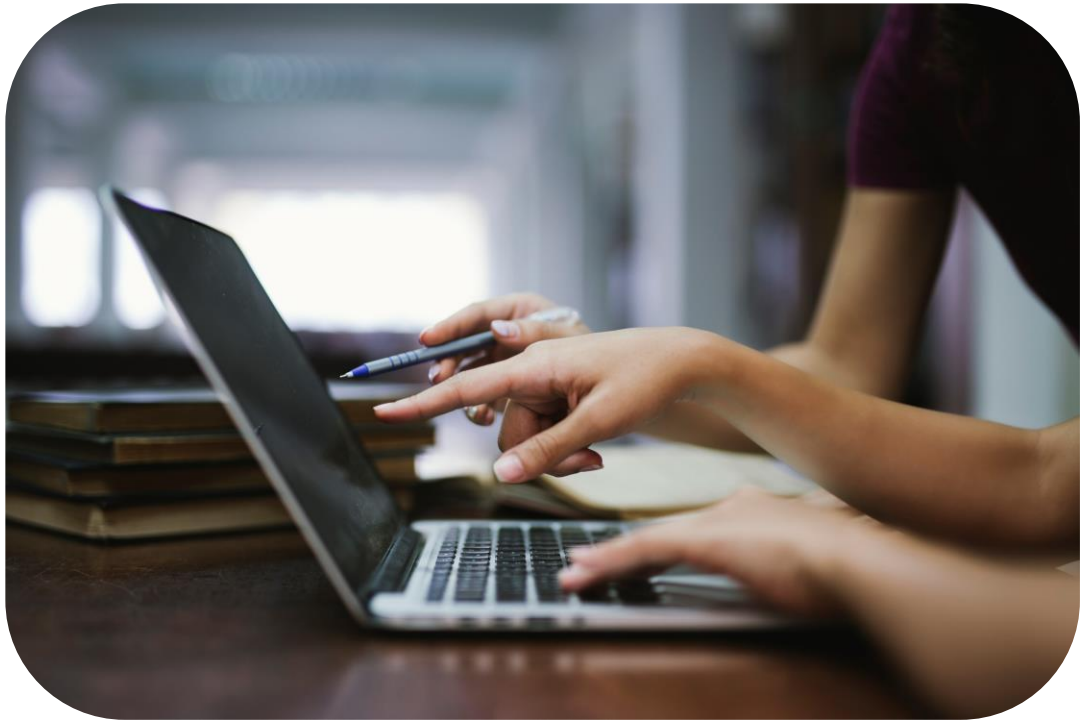
These data breaches resulted in financial and reputational damage to these companies.

Company	Number of customers affected	What happened?
Yahoo!	3 billion	Data was hacked by a “state-sponsored actor”.
Facebook	540 million	Published by Facebook developers.
Marriott	500 million	Legacy/old systems were able to be hacked.
Equifax	147 million	Hackers spotted software that hadn’t been updated and used this to help them access the data.
Capital One	100 million	Data hacked by former Amazon Web Service (AWS) employee.

More organisational data breaches

Data breaches often happen because,

- employees **don't realise the impact** of sharing information
- people have **not updated software** on their devices
- companies continuing to use **old/legacy systems** that are vulnerable to attacks
- companies working **unlawfully**



Hackers can then use these errors to help them access the information.

If you are working for an organisation that uses data, **you have a responsibility to keep that data safe**.

Show me…

Online fitness tracker Strava legally published “heatmaps” that showed the **paths that its users had run or cycled**.

This data did not contain any personal details. It appeared to be an interesting use of their data that could be benefit its users.

However, the fitness trackers were being used by the US military. This meant the heat maps showed **undisclosed locations of military bases and routes taken by soldiers**, which put the personnel at risk of attack.

The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan (BBC article Jan 2018)

https://www.bbc.co.uk/news/technology-42853072

Show me…

In May 2022, Facial recognition company Clearview AI was fined £7.5million for **illegally using images of British people scraped from the internet.** The company illegally set up a database of 20 billion faces without the individual's knowledge or permission.

Clearview AI was then offering an app where you could **upload a photo to try and identify the person against this unlawful database**.

As well as being fined, the company was ordered to stop obtaining data of UK residents and to delete the data they had already collected.

news.sky.com/story/facial-recognition-company-clearview-ai-fined-7-5m-for-illegally-using-images-of-brits-scraped-from-online

Next steps

Complete **questions 1 to 6**
in **section 1** of the
‘Keeping organisational data secure’ workbook.

How the law can protect your data

We have seen that companies don't always look after the data they hold on individuals in ways you might expect.

Now, we are going to look at the **laws that protect our data** and how they make it clear what **organisations can and cannot do with it.**

Definition

GDPR

Regulations (UK & EU) that govern the way that organisations can use, process and store personal data

GDPR - what are your data rights?

Right to be informed

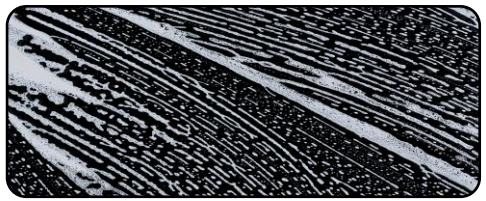
Individuals know at the point of data collection, what information is being collected, what it is being used for, why that information is required and how long that will be kept.

Right of access

Individuals can ask to see what data is held on them.

Right to rectification

If data is incorrect/incomplete, individuals have the right to ask for it to be fixed or updated



Right to erasure

Also known as the right to be forgotten, individuals can ask for personal data to be erased.

GDPR - what are your data rights?

Right to restrict processing

The data can be stored, but individuals can ask to limit how their data is used

Right to data portability

Individuals are allowed to move their data between different providers. e.g. smart meters

Right to object

It is possible to object to data being processed. e.g. unsubscribing from a newsletter.

Rights in relation to automated decision making and profiling

It is possible to ask to speak to a person, rather than have automated decisions made about an individual e.g. when applying for a credit card

What this means for you…

If a company holds personal data about you it has to be,

- **Accurate**
- Only used for the reason **you agreed** to
- **Deleted if you ask**
- You can **move data** between providers (such as wearable devices)
- **You can ask to see** what they hold on you

Companies use privacy notices to explain how they will use your personal data.

Definition

Privacy notice

Information that tells individuals how an organisation will use, store or share their personal data

Show me…

Here are **examples of privacy notices** from the National Portrait Gallery and the BBC.

National Portrait Gallery

Child and Young People Friendly Privacy Notice

What is a privacy notice

A Privacy Notice tells you what personal data the Gallery collects about you, how we use it and what you can do about it. **Personal data** means any information that can be used to identify you, such as your name, address or picture. This privacy notice is designed to be read by children and young people; you might want to read it with your parents, guardians, or a teacher. If you still have questions, you can ask us at the Gallery. View our more detailed Privacy Notice.

Who are we

Since 1856 the National Portrait Gallery has collected and displayed pictures of people who have contributed to British history and culture. You can find out more about how the Gallery works, our contact details and much more.

https://www.npg.org.uk/about/gallery-planning-and-policies/child-and-young-people-friendly-privacy-notice

Privacy Notice for Children's Uploads - 13 and Older

Page updated: 31 January 2020

We want to let you know that your information is safe with us. This is just a quick word to let you know how we handle your information when you send your creation to us.

What information about me do you ask for?

We might ask for information about you like your first name, age and hometown.

You might give us information about you in the creation you send to us. Sometimes we might be able to tell who you are if you send us a photo or video that you are in.

Please don't give us private information about you or your friends or family.

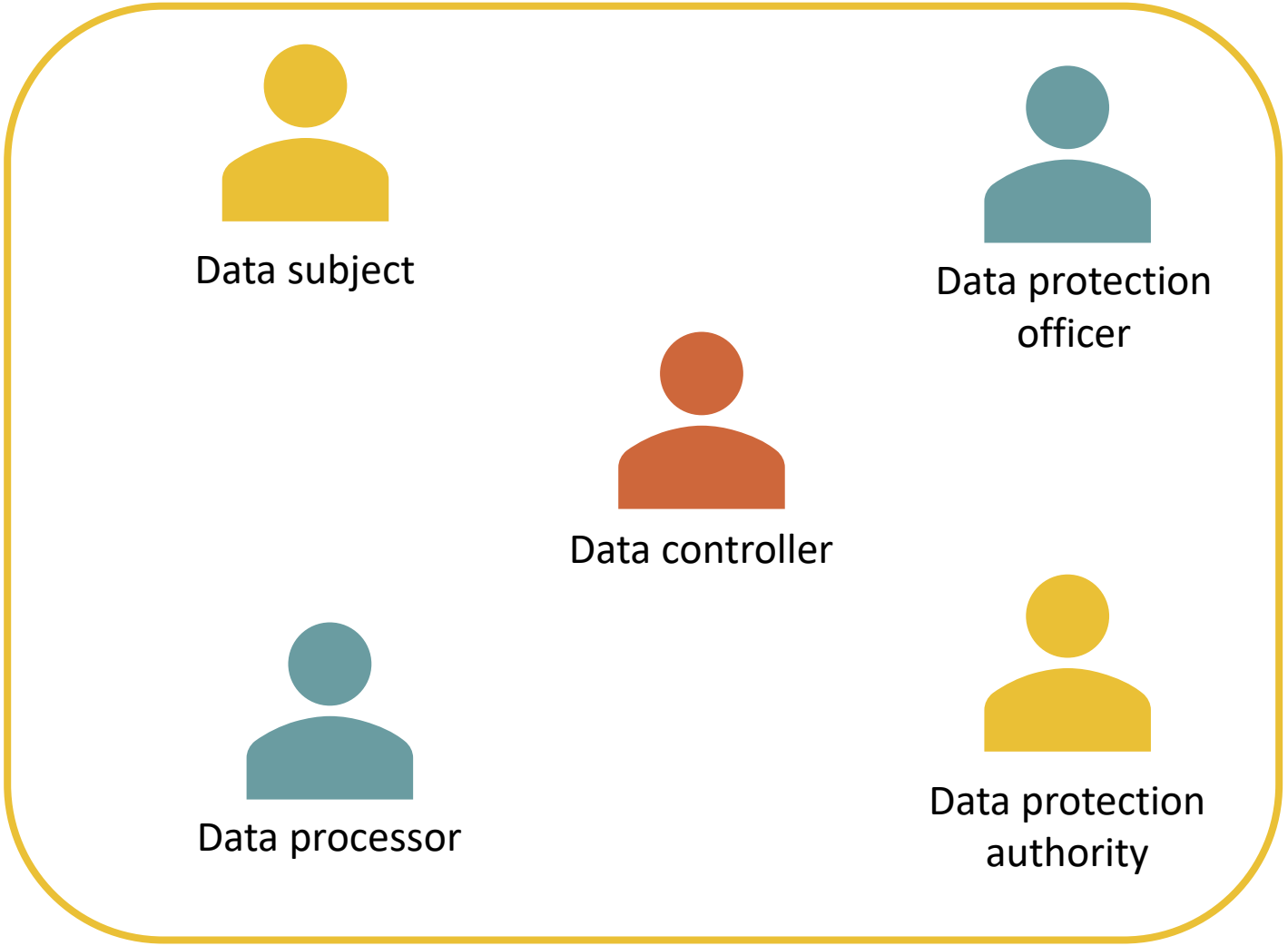
https://www.bbc.co.uk/usingthebbc/privacy/childrens-uploads-privacy-notice-13

Roles within GDPR

Within GDPR there are many different roles described, and their associated rights and responsibilities.

We are going to look at the roles of

- **Data subject**
- **Data controller**
- **Data processor**



Definition

Data subject

The identified or identifiable living individual to whom the personal data relates.

Definition

Data controller

Determines why and how personal data is processed in an organisation

Definition

Data processor

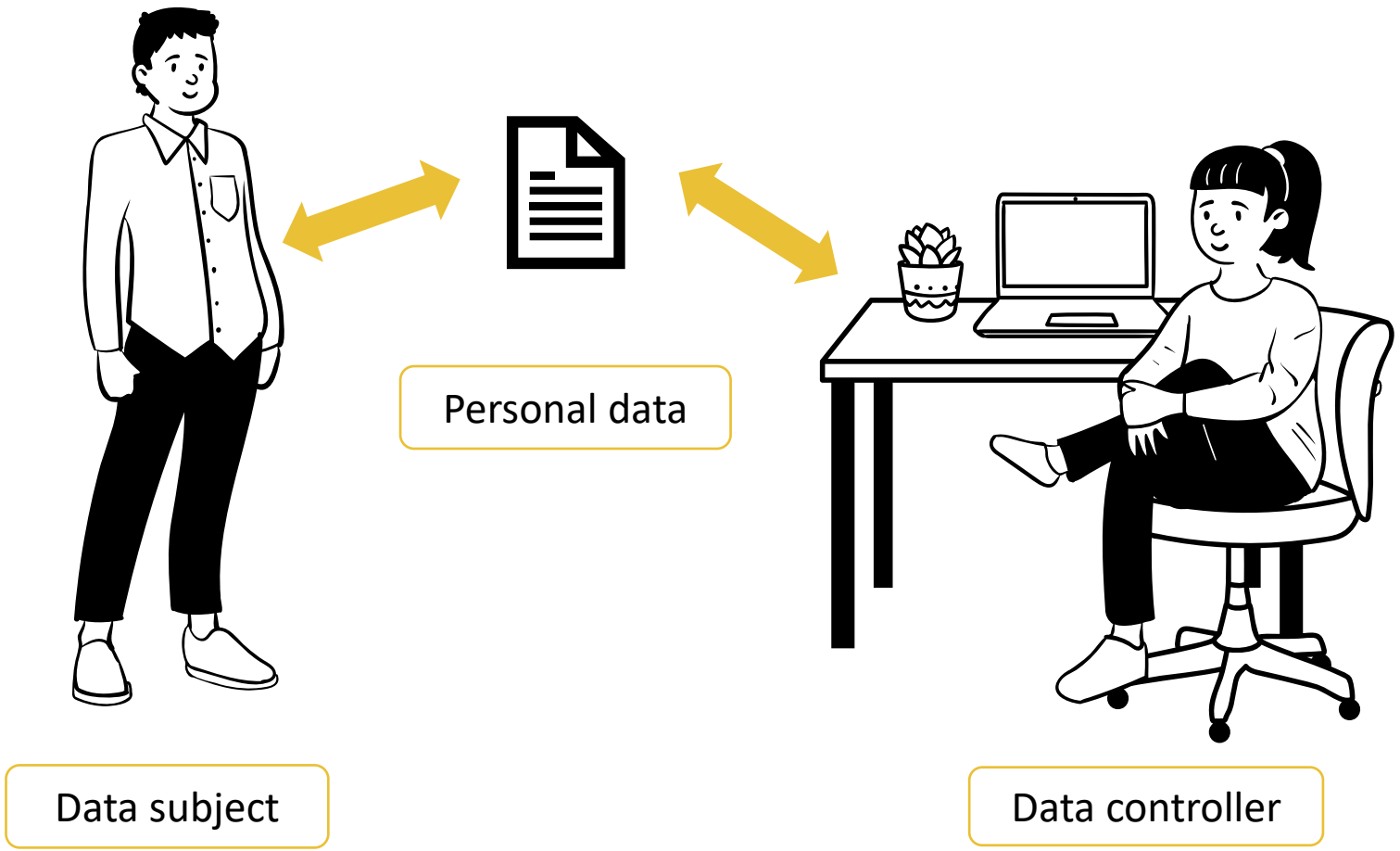
Processes the personal data on behalf of the controller

Show me…

Any time an organisation holds your personal data, you are a **data subject**.

The person who decided how the data is used within the organisation is the **data controller**.

The **data processor** will follow the instructions of the data controller to process the data.



Subject access request

Individuals can ask to see what data is held on them. This is called a **Subject Access Request**.

You can make a subject access request to find out:

- what personal information an organisation holds about you
- how they are using it
- who they are sharing it with
- where they got your data from

Companies should not charge a fee and should deal with the request within one month.

Dear Sir/Madam,

SUBJECT ACCESS REQUEST

I am writing to make a subject access request.

Full name:
Address:
Email address:

Please supply the data about me I am entitled to under data protection law including:

Your turn…

As a data subject, you can submit a subject access request to any organisation that holds your data.

What organisations can you think of that you could **submit a subject access request** to?

Your turn…

Here are some organisations you could submit a subject access request to,

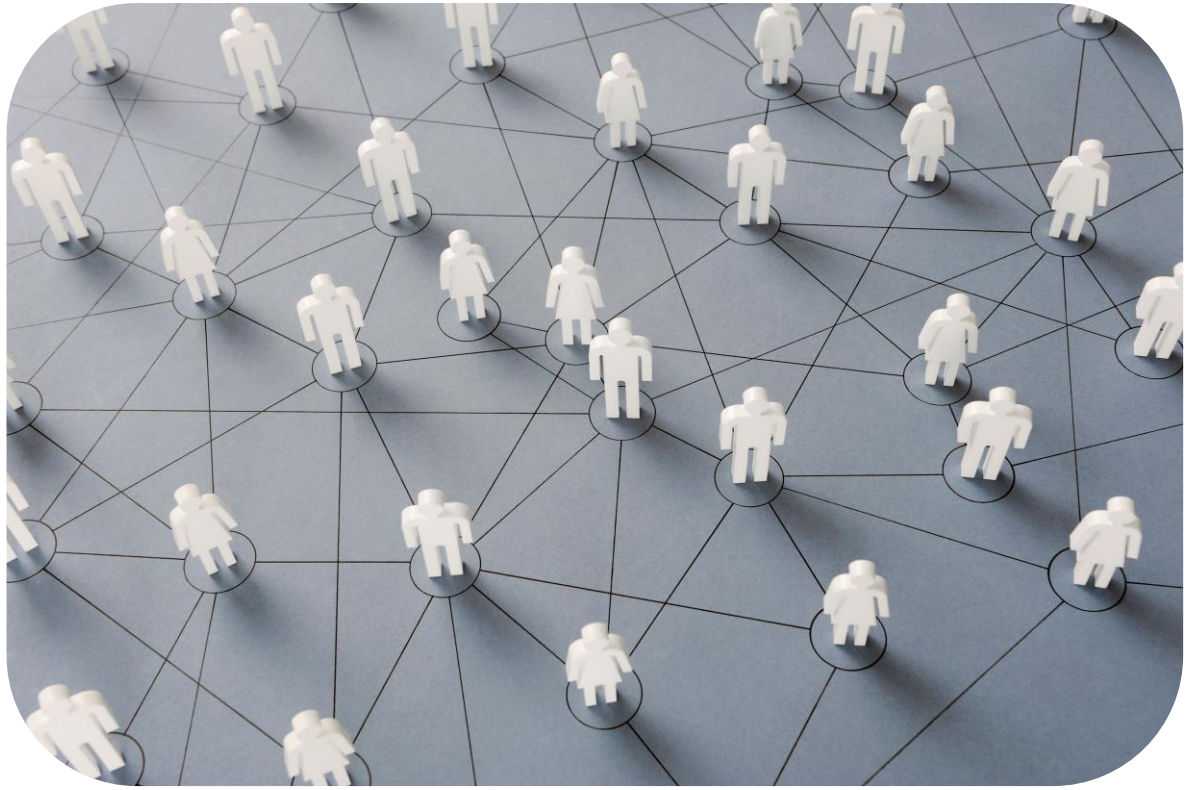
- Doctors
- School/college/employer
- Mobile phone company
- Social media company
- Bank

More on GDPR

As a data subject you have the right to check the information that an organisation is correct. If it's not accurate, you can **ask for it to be corrected**.

You also have the right to have ask for your data to be deleted if it is not required any more. Often referred to as the **right to be forgotten**, individuals can ask for **personal data to be erased.**

This request may be refused in certain circumstances e.g. for crime prevention, financial security, public health concerns or freedom of information.



Show me…

Here is a template letter from the information commissioner's office (ico) you can use if you wish to contact an organisation to have your personal data deleted.

[Your full address]
[Phone number]
[The date]

[Name and address of the organisation]
[Reference number (if applicable)]

Dear [Sir or Madam / name of the person you have been in contact with]

Right to erasure

[Your full name and address and any other details such as account number to help identify you]

I wish to exercise my right of erasure under data protection law.
[Give details of what personal data you want erased/deleted.]
You can find guidance on your obligations under information rights legislation on the website of the Information Commissioner's Office (www.ico.org.uk) as well as information on their regulatory powers and the action they can take.
Please send a full response within one calendar month confirming if you will comply with my request. If you cannot respond within that timescale, please tell me when you will be able to respond.

If there is anything you would like to discuss, please contact me.
Yours faithfully
[Signature]

Your turn…

Think about any organisations that **you have given your personal data** to in the past.

Are there any that you could contact to delete your personal data (under the right to erasure)?

Your turn…

Here are some examples of places you might want to contact to get your personal data deleted,

- After you have cancelled your **gym membership**, they no longer need a record of your health conditions
- **Social media or gaming apps** you used as a child
- **Magazine subscription** that you have cancelled, they no longer need your address

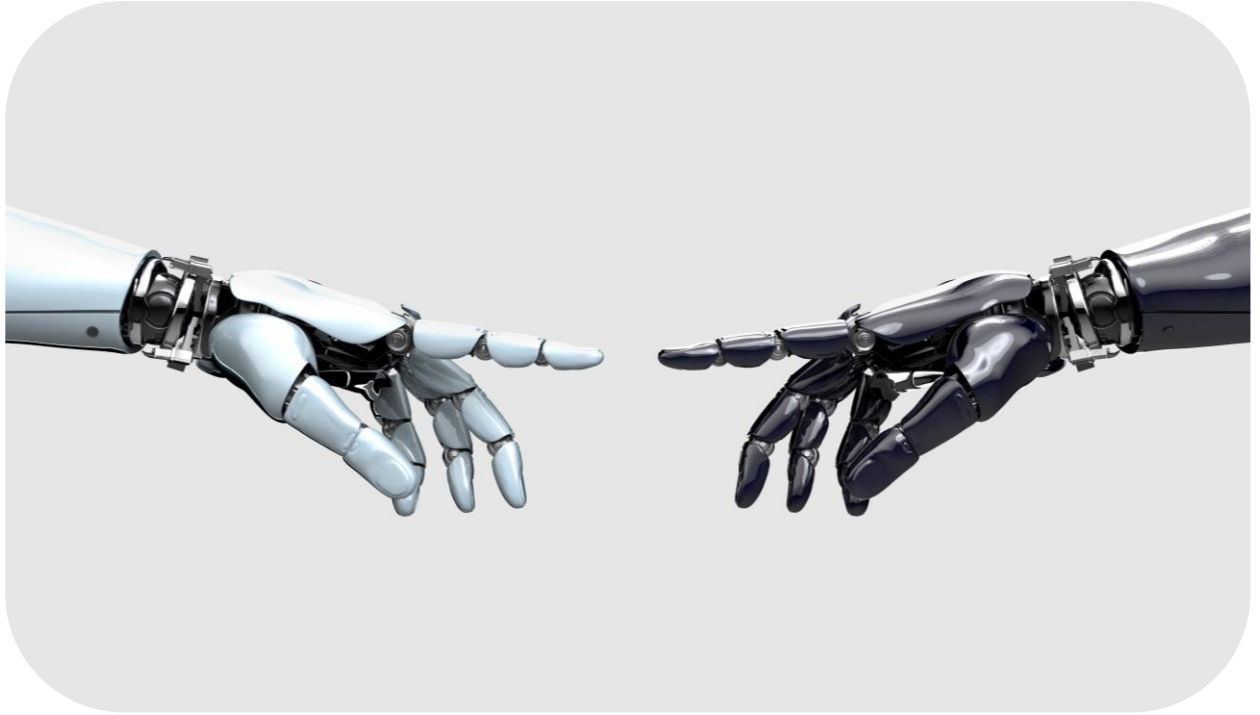
Next steps

Complete **questions 1 to 5**
in **section 2** of the
‘Keeping organisational data secure’ workbook.

What technology can be used to protect data

Organisations can **use technology to help them protect your data** and to make sure it is stored securely.

We are now going to look at some of these tools.



Definition

Encryption

To conceal the content of a message to prevent unauthorised people from reading it

Show me…

Encryption means that information such as text or data is encoded using a key and cannot be understood until it is decoded by another key other end of the information transfer.

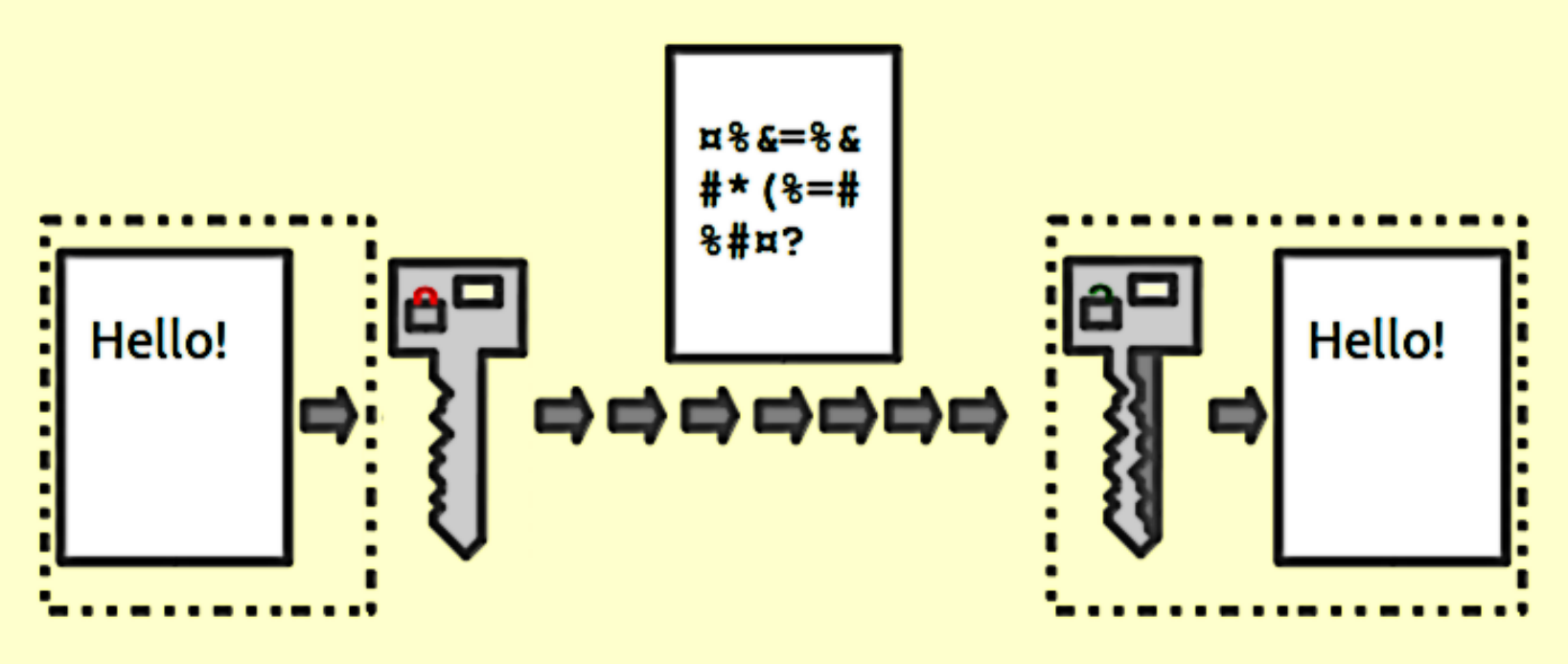


Illustration of how encryption is used within servers Public key encryption from Encryption Facts for Kids Kiddle Encyclopedia.

Encryption at rest and in transit

The main way to keep data safe is to encrypt it. It should be encrypted at rest and in transit.

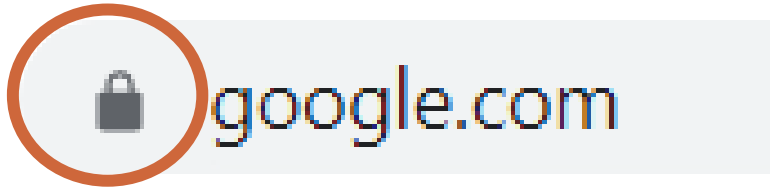
Data	Example	Why?
At rest 	When stored on a laptop	If the storage device is stolen or accessed, it can't necessarily be read.
In transit 	When being sent over email	It can't be intercepted en-route, for example on an open wifi connection.

How to identify encrypted sites

It is easy to identify if webpages are encrypted, since they have a web address starting with **https** rather than http.

They will also show a **locked padlock** next the website address.

It is important to ensure that when personal data is captured in a web form, the website is always **https** so that the data is encrypted in transit.



More ways organisations can protect data

Backing up data and code

- Data can sometimes be lost accidentally, either through deletion or corruption.
- Data should be backed up at regular intervals.

Limiting access

- Limit the users that have access to the data.
- Good practice to provide access to named individuals who have a valid reason.

Testing and monitoring

- Penetration testing is an ethical hacking test to identify weaknesses in security.
- Ongoing system monitoring to identify unauthorised data breaches.

Next steps

Complete **questions 1 to 3**
in **section 3** of the
‘Keeping organisational data secure’ workbook.

Learning checklist

I can *describe* how GDPR supports organisations to manage and secure data.

I can *describe* the rights I have as a data subject.

I can *describe* the responsibilities an organisation has a data controller.

I can *describe* how encryption can be used to manage and secure data.

How you can use this lesson

You are free to:

- **Share** – copy and redistribute the material in any medium or format
- **Adapt** – remix, transform and build upon the material

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** — You may not use the material for commercial purposes.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Created by Effini in partnership with Data Education in Schools and Skills Development Scotland.

Effini

Data Education in Schools

Skills Development Scotland

Alternative format

If you require this document in an alternative format, such as large print or a coloured background, please contact

hello@effini.com

or

4th Floor, The Bayes Centre
47 Potterrow
Edinburgh
EH8 9BT

Effini

Data Education in Schools

Skills Development Scotland