



Giving Consent and Responsibilities

Processing of Personal Data

Giving consent to process personal data

The threshold for consent to use of individuals' data is much higher than the previous Data Protection Act.

Any request for consent must be very clear, easy to read and in a plain language that the data subject can understand.

In practice, if consent is needed to collect and use your personal data, it is likely that an express opt-in will be the least that is required.

Consent:

01

Can be withdrawn at any time (and it must be easy to do so)

02

Is not always appropriate (eg if data would be processed anyway)

03

Won't be valid if there is too much of an imbalance of power (eg if an employer asks an employee for consent, the employee may feel obliged to grant it even if they do not want to)

04

Needs to remain valid (meaning it may need to be asked for again after a given period of time)

Responsibilities of organisations

The GDPR also applies to companies that process and control personal data.

It divides individuals and organisations into two categories - a Controller, and a Processor.

- ▶ Article 5 of the GDPR states the main principles of the act.
- ▶ Personal data shall be:
 - ▶ processed lawfully, fairly and transparently
 - ▶ only collected and used for lawful purposes
 - ▶ adequate, relevant and not excessive for that purpose
 - ▶ accurate and up to date
 - ▶ stored no longer than necessary
 - ▶ kept secure, and its integrity and confidentiality protected

Controller	Processor
Determines for what purpose the personal data is being used.	Needs to follow a specific set of legal obligations placed on them by the GDPR.
Responsible for making sure the Processor is complying with the GDPR	Maintain records of personal data, and the processing activities carried out on that data.
	Has the legal liability and it is them that is responsible if there is a data breach



Accountability

There is also a new accountability principle, which means companies and organisations need to be able to demonstrate compliance with these principles.

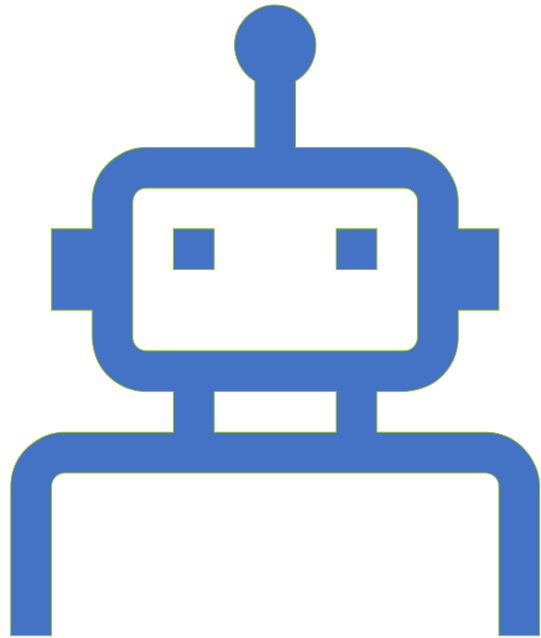
Data stored outside Europe

Our data is stored across many countries.

Cloud-based storage means that our personal data can now be stored on a server in a country outside of Europe.

Countries outside of Europe may have very different laws to our own when it comes to keeping data secure.

The GDPR states that data can only be transferred to a country, or international organisation, when an adequate level of protection is guaranteed.



Task

Now do Task 8