

Principles of Data Privacy

What is Data Privacy?

Data privacy is the right to control who gets to see your personal information; while Data security involves protecting data from unauthorized access, breaches, and theft.



Alt text: Data security concept

Data Privacy Principles

There are seven key principles of Data Privacy:



Lawfulness, Fairness, and Transparency

- This principle emphasises the importance of collecting and processing data in a legal and ethical manner.
- Organisations must have a legitimate reason for collecting data and be transparent about how it will be used.
- Individuals should be informed about what data is being collected, why it is collected, and their rights regarding that data.

Example:

A company collecting email addresses for a newsletter signup should clearly explain how the email addresses will be used and provide an option to unsubscribe at any time.

Purpose Limitation

This principle dictates that data should only be collected for specific, predetermined purposes and not be used for any other purpose without the individual's consent.

Example:

A website collecting a phone number for order fulfilment should not use it for marketing purposes without explicit consent.

Data Minimization

This principle emphasises collecting the minimum amount of data necessary to achieve the intended purpose.

Example:

An e-commerce platform might only need a shipping address for delivery, not the customer's entire home address.

Accuracy

This principle ensures that personal data is accurate, complete, and up-to-date. Organisations must take steps to ensure the accuracy of their data and allow individuals to correct any inaccuracies.

Example:

A company should allow users to update their contact information and preferences within their account.

Storage Limitation

This principle dictates that personal data should not be stored for longer than necessary to achieve the intended purpose. Organisations should have clear data retention policies and procedures for securely disposing of data when it is no longer needed.

Example:

A company might need to keep customer purchase history for a certain period for warranty purposes but should delete it after that time frame.

Integrity and Confidentiality

This principle focuses on protecting personal data from unauthorised access, disclosure, alteration, or destruction. Organisations must implement appropriate security measures to safeguard data privacy.

Example:

Using encryption for sensitive data and access controls to restrict access to authorised personnel.

Accountability

This principle emphasises that organisations are responsible for ensuring compliance with data privacy principles. Organisations must be able to demonstrate their adherence to these principles and address any data breaches or privacy violations.

Example:

Appointing a Data Protection Officer (DPO) and conducting regular privacy audits.