



INFORMATION PRIVACY LAW COURSE SERIES
Foundations and Themes of US Privacy Law

OECD PRIVACY GUIDELINES

Below is a summary of the Privacy Guidelines issued by the Organization for Economic Cooperation and Development (OECD):

Collection Limitation Principle

Data should be collected lawfully with the individual's consent.

Data Quality Principle

Data should be relevant to a particular purpose and be accurate, complete, and up to date.

Purpose Specification Principle

The purpose for data collection should be stated at the time of the data collection, and the use of the data should be limited to this purpose.

Use Limitation Principle

Data should not be disclosed for different purposes without the consent of the individual or the authority of law.

Openness Principle

Individuals should be informed about the practices and policies of those handling their personal information.

Security Safeguards Principle

Data should be protected by reasonable security safeguards.

Individual Participation Principle

People should be able to learn about the data that an organization possesses about them and to rectify errors or problems in that data.

Accountability Principle

The organizations that control personal information should be held accountable for carrying out these principles.

In 2013, three concepts were added to the OECD Privacy Guidelines:

National Privacy Strategies

There should be a multifaceted national strategy at the highest levels of government.

Privacy Management Programs

Organizations should have operational mechanisms to implement privacy protections.

Data Security Breach Notification

Individuals whose personal data is involved in data breach should be notified.