



INFORMATION PRIVACY LAW COURSE SERIES
**GDPR and European Privacy Law Part II:
GDPR Rights, Obligations, and Data Transfer**

EU-US PRIVACY SHIELD PRINCIPLES

1. Notice

Participating companies must provide individuals with a variety of different information including: (1) type of data collected, (2) purpose of collection, (3) circumstances of onward transfer, (4) third-party identities, (5) rights of the individuals, (6) redress channels for the individuals.

2. Choice

The Privacy Shield gives individuals a right to opt out of their information being disclosed to a third party, or used for a purpose that is materially different than the purpose for which it was originally collected or subsequently authorized by the individual. Opt-out mechanisms must be “clear, conspicuous, and readily available.”

3. Accountability for Onward Transfer

Organizations are liable for compliance with the Notice and Choice Principles when transferring information to a third party acting as a controller. To so, organization must enter into a contract with the third-party controller.

4. Security

Companies must take reasonable and appropriate measures to protect personal information taking into account the risks involved in the processing and the nature of the personal information.

5. Data Integrity and Purpose Limitation

Companies possess a duty to ensure that personal data held and processed by the organization is “reliable for its intended use, accurate, complete, and current.”

6. Access

Individuals are to have access to personal information about them and be able to correct, amend, or delete that information when it is inaccurate, or has been processed in violation of the Principles. Companies are to reply to individual complaints within 45 days.

7. Recourse, Enforcement and Liability

The Privacy Shield provides the right to file privacy complaints directly with participating companies. The agreement requires independent recourse mechanisms that must be free of charge to individuals.