GDPR

**TERITORIAL SCOPE**
- EU Establishments
- Non-EU Established Organizations
  - Offer goods or services or engaging in monitoring within the EU.

**LAWFUL PROCESSING**
- Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for
  - performance of a contract
  - compliance with a legal obligation
  - to protect a person’s vital interests
  - task in the public interest
  - legitimate interests

**CONSSENT**
- Consent must be freely given, specific, informed, and unambiguous.

**RIGHTS OF DATA SUBJECTS**
- Automated Decision Making
- Transparency
- Access and Rectification
- Right to Erasure
- Purpose Specification and Minimization
- Right to Data Portability
- "Right not to be subject to a decision based solely on automated processing, including profiling."

**ENFORCEMENT**
- Fines
  - Up to 20 million euros or 4% of total annual worldwide turnover.
  - Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.
  - Effective Judicial Remedies: compensation for material and non-material harm.
  - Binding Corporate Rules (BCRs)

**INTERNATIONAL DATA TRANSFER**
- Adequate Level of Data Protection
- Privacy Shield
- Model Contractual Clauses

**RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS**
- Data Protection Officer (DPO)
- Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.
- Record of Data Processing Activities
- Maintain a documented register of all activities involving processing of EU personal data.

**DATA BREACH NOTIFICATION**
- A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- If likely to result in a high privacy risk → notify data subjects
- Notify supervisory authorities no later than 72 hours after discovery.

**SENSITIVE DATA**
- Religious or Philosophical Beliefs
- Trade Union Membership
- Political Opinions
- Racial or Ethnic Origin
- Genetic Data
- Biometric Data
- Health

**PERSONAL DATA**
- Identified
- Identifiable

**TEACHPRIVACY**
- www.teachprivacy.com
- Workforce awareness training by Prof. Daniel J. Solove
- Please ask permission to reuse or distribute
PRIVACY AWARENESS TRAINING FOR GLOBAL ORGANIZATIONS

Impeccable Expertise
Our training is created by Professor Daniel Solove, one of the world’s leading privacy and security experts.

A Masterful Overview of Privacy
Professor Solove synthesizes key privacy concepts in a way that transcends particular jurisdictions.

Clear, Understandable, and Engaging
Masterful use of concrete examples, quiz questions, activities, games, and vignettes.

100+ privacy and security topics
Including GDPR, Privacy by Design, CASL, Privacy Shield, FAR Privacy Act, Online Advertising, HIPAA, Phishing, PCI, and much more.

See it for yourself: https://teachprivacy.com/
Contact us: inquiry@teachprivacy.com