COURSE

Global Data Privacy

3rd Edition   Ethics   🌐

Protect Personal Information and Comply with FIPPs

If your business tracks any type of personal information through products, services or promotion, global data privacy rules apply. Starting with Europe's GDPR in 2018, California's CCPA in 2020, Brazil's privacy regulation in 2020 and other emerging data privacy laws, it's impossible to conduct business today without clear and up to date information on the global guidelines for workplace data privacy training.

Course Description

This course teaches the basics of global data privacy training and workplace data security training. Instruct learners on your companies own data privacy policies, as well as the U.S. and European Union's data privacy laws and standards, such as Fair Information Protection Practices ("FIPPs"). We also address the consequences for violating data privacy practices and mishandling personal information.

Interactive polling questions in the course give employers real insight into how employees feel about the concepts and culture skills presented. Emtrain's innovative Ask the Expert feature gives learners direct access to course experts.

Key Concepts

- What data privacy is, what data security is, and what personal information is.
- The sources of data privacy rules, including employer policies, contracts, U.S. law and laws in the European Union.
- What Fair Information Protection Practices ("FIPPs") are and their role n the U.S. and around the globe.
- What the European Union's General Data Protection Regulation is, who it applies to and what it requires.
- What Binding Corporate Rules and Model Contract Clauses are.
- The penalties and consequences of mishandling personal information.

Course Features

- Access to our Anonymous Ask the Expert tool
- Rich video scenarios based on real-world events
- Built-in employee sentiment surveys
- 50+ Machine Translation Options
- Optional program timer
- Policy acknowledgement tool
- Extensive customization options

Lessons

Why Privacy Matters

Businesses collect enormous amounts of personal data — and how that data gets handled has real consequences. Explore the distinction between data privacy and data security, and why responsible data practices matter for legal compliance people behind the data.

PILLAR

Ethics (https://emtrain.com/products/ethics/)

VERSIONS

All Employees (35 min)

WHAT'S COVERED

- CCPA (California Consumer Privacy Act)
- CPRA (California Privacy Rights Act)
- Data Breach
- Data Incidents
- Data Privacy Vs. Data Security
- FIPP (Fair Information Practice Principles)
- GDPR (General Data Protection Regulation)
- Patient Records
- PHI (Protected Health Information)
- PII (Personal Identifiable Information)
- Privacy Laws
- Privacy Rule
- Security Incidents
- Security Rule

COURSE EXPERTS

Sharon Anolik

What Is Personal Information?

Recognizing personal information isn't always straightforward — data can identify someone directly, indirectly, or through combination with other details. Explore how personal and sensitive data are defined globally, and why understanding the difference matters in your day-to-day work.

Core Privacy Principles

From transparency and consent to data minimization and accountability, this lesson walks through the globally recognized Fair Information Practice Principles — and what they look like in practice across everyday work situations.

The Global Privacy Landscape

Privacy obligations aren't just best practices — they're enforceable requirements that vary by country, contract, and context. Survey the major global privacy frameworks, individual data subject rights, and the roles organizations play as data controllers and processors.

Lawful Basis, Consent, and Transparency

Processing personal data isn't as simple as collecting what's useful — organizations must have a valid legal basis, use consent appropriately, and be transparent with the people whose data they handle. Explore how these foundational requirements work in practice across global privacy frameworks.

The Information Lifecycle

Personal data doesn't just appear and disappear — it moves through a defined lifecycle, and each stage carries its own responsibilities. Explore the five phases of the information lifecycle and the key practices that keep personal data protected from collection through deletion.

Individual Rights

Modern privacy laws give individuals real control over their personal data — and organizations have concrete obligations when those rights are invoked. Explore the key individual rights recognized across global frameworks, how to handle data subject requests in practice, and what happens when things go wrong.

Data Sharing, Transfers, and Third-Party Obligations

Sharing personal data with vendors, partners, or across borders doesn't transfer your organization's responsibility for it. Explore the legal requirements around data sharing and cross-border transfers, what due diligence looks like in practice, and why third-party obligations don't end when the data leaves your hands.

AI and Privacy

AI tools offer real efficiency gains at work — but they also introduce serious privacy risks that aren't always obvious. Explore the dangers of data leakage and shadow AI, what responsible AI use looks like in practice, and how emerging regulations like the EU AI Act are raising the bar.

Privacy in Practice

Privacy isn't just a policy on a shelf — it has to be built into how we work every day. Explore practical privacy habits, the Privacy by Design approach, how to conduct Privacy Impact Assessments, and what to do when security incidents or data events occur.