Building a Global Privacy Program Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In an era of relentless digital transformation and increasing global scrutiny, establishing a robust Global Privacy Program is no longer optional it's a critical business imperative. The patchwork of evolving international regulations, from the GDPR and CCPA to Brazil's LGPD and China's PIPL, mandates a harmonized, risk-based approach to data governance. This specialized training empowers organizations and their key personnel to navigate this complex regulatory landscape, transforming compliance from a cost center into a source of competitive advantage and customer trust. Success hinges on the ability to operationalize privacy principles across diverse business units, jurisdictions, and technology stacks, ensuring accountability and the protection of Personally Identifiable Information (PII) worldwide.

Building a Global Privacy Program Training Course is designed to equip participants with the strategic vision and practical, operational toolkit necessary to design, implement, and maintain an effective, scalable, and future-proof privacy program. We focus on cutting-edge practices like Privacy by Design, advanced Privacy-Enhancing Technologies, and effective Cross-Border Data Transfer mechanisms. By emphasizing real-world case studies and a risk management framework, this program moves beyond mere legal checklist compliance to foster a sustainable Culture of Privacy. Graduates will master the art of integrating privacy into the product lifecycle, managing Data Subject Rights Requests at scale, and responding to data breaches with speed and regulatory confidence, ultimately securing the organization's reputation and bottom line.

Programme Curriculum

Building a Global Privacy Program Training Course

Introduction

In an era of relentless digital transformation and increasing global scrutiny, establishing a robust Global Privacy Program is no longer optional it's a critical business imperative. The patchwork of evolving international

regulations, from the GDPR and CCPA to Brazil's LGPD and China's PIPL, mandates a harmonized, risk-based approach to data governance. This specialized training empowers organizations and their key personnel to navigate this complex regulatory landscape, transforming compliance from a cost center into a source of competitive advantage and customer trust. Success hinges on the ability to operationalize privacy principles across diverse business units, jurisdictions, and technology stacks, ensuring accountability and the protection of Personally Identifiable Information (PII) worldwide.

Building a Global Privacy Program Training Course is designed to equip participants with the strategic vision and practical, operational toolkit necessary to design, implement, and maintain an effective, scalable, and future-proof privacy program. We focus on cutting-edge practices like Privacy by Design, advanced Privacy-Enhancing Technologies, and effective Cross-Border Data Transfer mechanisms. By emphasizing real-world case studies and a risk management framework, this program moves beyond mere legal checklist compliance to foster a sustainable Culture of Privacy. Graduates will master the art of integrating privacy into the product lifecycle, managing Data Subject Rights Requests at scale, and responding to data breaches with speed and regulatory confidence, ultimately securing the organization's reputation and bottom line.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Assess Global Data Privacy Regulations and their impact on multinational operations.
2. Design a Risk-Based Privacy Framework leveraging NIST and ISO standards.
3. Implement Privacy by Design and Default principles into product development and business processes.
4. Conduct comprehensive Data Protection Impact Assessments and Transfer Impact Assessments.
5. Establish a clear global Data Governance Model and Record of Processing Activities.
6. Operationalize efficient Data Subject Rights request fulfillment across jurisdictions.
7. Manage and secure Cross-Border Data Transfers using SCCs, Binding Corporate Rules, and adequacy decisions.
8. Develop and execute an effective Data Breach Incident Response Plan with regulatory notification protocols.
9. Integrate AI Governance and Ethical Data Use into the corporate privacy strategy.
10. Define, track, and report on key Privacy Program Metrics for executive visibility.
11. Audit and manage Third-Party Vendor Risk and supply chain privacy compliance.
12. Select and deploy relevant Privacy-Enhancing Technologies like anonymization and pseudonymization.
13. Foster a sustainable, measurable Culture of Privacy Awareness and employee accountability.

Target Audience

1. Chief Privacy Officers and Data Protection Officers.
2. Privacy/Compliance Managers and Analysts.
3. Legal Counsel and Regulatory Affairs Professionals.
4. Information Security and IT Directors.
5. Product Managers and Engineers.
6. Internal Auditors and Risk Managers.
7. HR and Marketing Executives.
8. Senior Executives and Board Members.

Course Modules

Module 1: The Global Privacy Imperative and Strategy

- The strategic value of privacy.
- Mapping the global regulatory patchwork.
- Defining the Privacy Program Scope, Charter, and Accountability Structure
- Developing a Privacy Vision aligned with organizational values and business goals.
- Aligning the program with established frameworks
- Case Study: Global Telecom Giant Fined for Inadequate Privacy by Design.

Module 2: Foundational Data Governance and Inventory

- Identifying and classifying Personally Identifiable Information and sensitive data.
- Creating and maintaining a global Record of Processing Activities
- Implementing Data Minimization and Purpose Limitation policies.
- Developing global Data Retention and Disposal schedules.
- Establishing a Data Flow Mapping and visualization process.
- Case Study: Healthcare Company's Breach from Retaining Stale, Unnecessary PII.

Module 3: Privacy by Design and Impact Assessments

- The seven foundational principles of Privacy by Design and Privacy by Default.
- Methodology for conducting Data Protection Impact Assessments.
- Integrating DPIAs into the Software Development Lifecycle.
- Embedding Privacy into new business initiatives and technology procurement.
- Risk scoring and mitigation planning based on DPIA outcomes.
- Case Study: Launching a New Product Without a DPIA, Leading to Feature Redesign Post-Launch.

Module 4: Data Subject Rights (DSR) Management

- Understanding the full spectrum of global Data Subject Rights
- Designing and implementing a scalable DSR Fulfillment Workflow.
- Verification of identity and handling of complex/vexatious requests.
- Legal grounds for refusing or restricting DSRs.
- Automating DSR discovery and response across disparate systems.
- Case Study: The Challenge of Fulfilling a "Right to Erasure" Request in Legacy Systems.

Module 5: Cross-Border Data Transfers

- Core mechanisms for legitimate international data transfer
- Conducting Transfer Impact Assessments based on Schrems II and evolving guidance.
- Managing compliance in high-risk jurisdictions
- Technical and organizational supplementary measures
- Data Localization, Residency, and Sovereignty requirements.
- Case Study: A Multinational Company Forced to Suspend EU-US Data Transfers After Regulatory Challenge.

Module 6: Third-Party and Vendor Risk Management

- Developing a risk-based Vendor Due Diligence and assessment program.
- Negotiating and managing Data Processing Agreements and liability clauses.

- Implementing ongoing monitoring and audit rights for third parties.
- Managing Nth-Party Risk in the data supply chain.
- Terminating contracts and ensuring secure data disposal by vendors.
- Case Study: A Major Supply Chain Breach Originating from a Low-Tier, Unmonitored Vendor.

Module 7: Incident Response and Crisis Management

- The difference between a security incident and a Personal Data Breach.
- Developing a global, coordinated Incident Response Plan and breach management team.
- Global regulatory Breach Notification Requirements
- Forensics, root cause analysis, and post-incident remediation.
- Conducting tabletop exercises and breach simulation drills.
- Case Study: Retail Company's Delayed Notification and the Resulting Regulatory Fine and Class Action.

Module 8: Program Measurement, Auditing, and Future Trends

- Defining Privacy Program Metrics and reporting to the Board/Executive Leadership.
- Conducting internal and external Privacy Audits and gap analysis.
- Training and awareness programs.
- The nexus of AI, Machine Learning, and Privacy
- Decentralized Identity, tokenized consent, and new consumer rights.
- Case Study: Leveraging AI Impact Assessments to Mitigate Ethical and Privacy Risks in a New ML Product.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com