Training Course on Data Breach Notification Laws and Compliance

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As data becomes the backbone of the digital economy, breaches in data security can have catastrophic implications—legally, financially, and reputationally. Training Course on Data Breach Notification Laws and Compliance is a high-impact, industry-focused program designed to equip professionals with the legal knowledge and compliance strategies required to effectively respond to data breaches. From understanding GDPR and CCPA to responding to cyber incidents with confidence, this course delves into the global regulatory landscape, helping organizations mitigate risk, avoid penalties, and maintain customer trust.

In an era of rising cyberattacks, ransomware, and strict privacy mandates, professionals must be prepared to handle breach notification requirements promptly and correctly. This course offers expert insights into cross-border data protection laws, incident response plans, data risk assessments, and regulatory reporting obligations. Whether you're in IT, legal, risk, or compliance roles, mastering breach notification compliance is essential for protecting sensitive data and maintaining operational integrity.

Programme Curriculum

Training Course on Data Breach Notification Laws and Compliance

Introduction

As data becomes the backbone of the digital economy, breaches in data security can have catastrophic implications—legally, financially, and reputationally. Training Course on Data Breach Notification Laws and Compliance is a high-impact, industry-focused program designed to equip professionals with the legal knowledge and compliance strategies required to effectively respond to data breaches. From understanding GDPR and CCPA to responding to cyber incidents with confidence, this course delves into the global regulatory landscape, helping organizations mitigate risk, avoid penalties, and maintain customer trust.

In an era of rising cyberattacks, ransomware, and strict privacy mandates, professionals must be prepared to handle breach notification requirements promptly and correctly. This course offers expert insights into cross-border data protection laws, incident response plans, data risk assessments, and regulatory reporting obligations. Whether you're in IT, legal, risk, or compliance roles, mastering breach notification compliance is essential for protecting sensitive data and maintaining operational integrity.

Course Objectives

1. Understand global data breach notification laws (GDPR, HIPAA, CCPA).
2. Identify key components of a breach response strategy.
3. Assess the legal implications of cybersecurity incidents.
4. Learn cross-border breach notification procedures.
5. Map out data flow to identify high-risk touchpoints.
6. Build effective incident response workflows.
7. Execute timely reporting to regulatory bodies.
8. Differentiate between notifiable and non-notifiable breaches.
9. Analyze breach severity using risk-based frameworks.
10. Ensure compliance with sector-specific regulations (financial, healthcare, education).
11. Integrate data protection policies with compliance programs.
12. Review real-world breach cases to identify best practices.
13. Evaluate organizational readiness through breach simulation exercises.

Target Audience

1. Data Protection Officers (DPOs)
2. IT and Cybersecurity Managers
3. Corporate Compliance Officers
4. In-house Legal Counsel
5. Risk Management Professionals
6. Government and Regulatory Liaisons
7. Privacy Consultants
8. Healthcare and Financial Services Compliance Teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Data Breach Laws

- Definition of a data breach.
- History and evolution of data privacy regulations.
- Global overview: GDPR, CCPA, HIPAA, and others.
- Key terms and definitions.
- Roles of different stakeholders in compliance.
- **Case Study: Equifax Data Breach and Legal Fallout.**

Module 2: Breach Notification Requirements

- Timelines for breach notifications by jurisdiction.
- What triggers a notification?
- Reporting thresholds and exceptions.
- Notifications to individuals, regulators, and partners.
- Penalties for non-compliance.
- **Case Study: Marriott Breach & GDPR Violation Fines.**

Module 3: Identifying and Assessing a Breach

- Steps in breach detection.
- Breach vs. security incident.
- Tools for breach identification.
- Evaluating breach severity and impact.
- Internal escalation procedures.
- **Case Study: Capital One Cloud Misconfiguration Breach.**

Module 4: Building a Breach Response Plan

- Incident response team roles.
- Communication strategy post-breach.
- Coordination with legal and public relations.
- Testing and updating the plan.
- Integration with business continuity plans.
- **Case Study: Uber Breach Cover-Up and Legal Consequences.**

Module 5: Regulatory Reporting Frameworks

- GDPR Article 33 and 34 overview.
- CCPA notification timeline.
- Country-specific reporting variations.
- Creating documentation trails.
- Working with Data Protection Authorities (DPAs).
- **Case Study: TikTok Regulatory Investigations (Europe & US).**

Module 6: Sector-Specific Regulations

- HIPAA breach notification rule (healthcare).
- GLBA and FFIEC guidelines (financial sector).
- FERPA in education data breaches.
- PCI DSS for payment data.
- Compliance overlap and conflict resolution.
- **Case Study: Anthem Healthcare Breach Response.**

Module 7: Cyber Insurance and Legal Liability

- Coverage for breach notification costs.
- Subrogation and third-party liability.
- Legal counsel’s role during breach handling.
- Indemnity clauses and contract reviews.
- Negotiating settlements and fines.
- **Case Study: Target’s Cyber Insurance Payout & Liability.**

Module 8: Cross-Border Data Breach Management

- Multi-jurisdictional breach obligations.
- Data localization laws.
- Working with international regulators.
- Harmonizing compliance processes.
- Managing time zone and language barriers.
- **Case Study: Facebook Cambridge Analytica Scandal.**

Module 9: Breach Communication Strategies

- Drafting breach notification letters.

- Communicating with regulators.
- Managing customer trust post-breach.
- Media and press release planning.
- Social media and crisis control.
- **Case Study: Zoom Data Leak and Public Response.**

Module 10: Risk Assessment & Mitigation

- Data flow mapping and risk identification.
- Risk scoring for breach readiness.
- Applying NIST and ISO 27001 standards.
- Prioritizing risk treatment actions.
- Regular audit and assessment schedules.
- **Case Study: JP Morgan Risk Gaps & Audit Findings.**

Module 11: Internal Policies & Training

- Employee awareness programs.
- Breach simulation exercises.
- Creating a data governance framework.
- Policy documentation and enforcement.
- Handling insider threats.
- **Case Study: Edward Snowden NSA Data Breach.**

Module 12: Legal and Ethical Considerations

- Ethical duties in breach response.
- Whistleblower protections.
- Balancing transparency with liability.
- Legal hold and litigation readiness.
- Global privacy ethics frameworks.
- **Case Study: Apple vs. FBI Data Privacy Dispute.**

Module 13: Technologies for Breach Prevention

- Intrusion detection and prevention systems.
- Encryption and anonymization techniques.
- Endpoint protection.
- Data loss prevention (DLP) tools.
- Automated breach reporting tools.
- **Case Study: LinkedIn Breach & Encryption Failure.**

Module 14: Preparing for Regulator Audits

- Pre-audit checklists.
- Mock regulatory interviews.
- Documentation for audit readiness.
- Responding to audit findings.
- Post-audit improvement plans.
- **Case Study: Google GDPR Audit in France.**

Module 15: Capstone Breach Simulation & Assessment

- Full-scale breach scenario simulation.
- Real-time decision-making exercise.
- Cross-functional response evaluation.

- Reporting templates and mock notifications.
- Final compliance audit by trainer.
- **Case Study: Multi-National Simulated Breach Drill.**

Training Methodology

- Interactive instructor-led virtual/live sessions.
- Real-world case studies and breach simulations.
- Role-play and scenario-based group exercises.
- Compliance checklists, reporting templates, and audit tools.
- Pre- and post-assessment quizzes for skill evaluation.

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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