Managing Data Breaches Under Global Regulations 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

The proliferation of global data privacy laws including GDPR, CCPA/CPRA, LGPD, and others has transformed a security incident into a major legal and financial crisis. Today, a data breach is no longer just an IT or cybersecurity challenge; it's an existential compliance risk demanding an orchestrated, cross-functional, and legally sound response. Organizations face unprecedented scrutiny, with potential fines reaching into the hundreds of millions and irreparable reputational damage. The difference between a controlled incident and a catastrophic failure lies in the maturity of the Incident Response Plan and the specialized training of the personnel executing it.

Managing Data Breaches Under Global Regulations Training Course provides the critical knowledge and actionable framework necessary to navigate the complex web of global breach notification mandates and regulatory obligations. Participants will master a seven-stage, best-practice methodology for breach management, from the critical initial hours of incident triage and containment to the final stages of regulatory reporting, evidence preservation, and post-incident remediation. By integrating legal requirements with technical response strategies, the course ensures your team can minimize financial penalties, maintain data subject trust, and demonstrate accountability to supervisory authorities worldwide. This is essential training for achieving cyber resilience in a heavily regulated digital landscape.

Programme Curriculum

Managing Data Breaches Under Global Regulations Training Course

Introduction

The proliferation of global data privacy laws including GDPR, CCPA/CPRA, LGPD, and others has transformed a security incident into a major legal and financial crisis. Today, a data breach is no longer just an IT or cybersecurity challenge; it's an existential compliance risk demanding an orchestrated, cross-functional, and

legally sound response. Organizations face unprecedented scrutiny, with potential fines reaching into the hundreds of millions and irreparable reputational damage. The difference between a controlled incident and a catastrophic failure lies in the maturity of the Incident Response Plan and the specialized training of the personnel executing it.

Managing Data Breaches Under Global Regulations Training Course provides the critical knowledge and actionable framework necessary to navigate the complex web of global breach notification mandates and regulatory obligations. Participants will master a seven-stage, best-practice methodology for breach management, from the critical initial hours of incident triage and containment to the final stages of regulatory reporting, evidence preservation, and post-incident remediation. By integrating legal requirements with technical response strategies, the course ensures your team can minimize financial penalties, maintain data subject trust, and demonstrate accountability to supervisory authorities worldwide. This is essential training for achieving cyber resilience in a heavily regulated digital landscape.

Course Duration

5 days

Course Objectives

1. Master the 72-hour notification clock for GDPR, CCPA/CPRA, and other major regulatory bodies.
2. Develop a risk-based assessment methodology for classifying incident severity and likelihood of harm to data subjects.
3. Operationalize a cross-functional Data Breach Incident Response Plan (DBIRP) aligned with NIST and ISO 27001 standards.
4. Differentiate between a Security Incident and a Personal Data Breach under GDPR Article 4(12).
5. Apply forensic-readiness techniques for effective evidence preservation and chain of custody?ƒöù management.
6. Understand the varying territorial scope and application of Extra-Territorial laws to global incidents.
7. Design legally compliant and transparent communication protocols for notifying data subjects and the public.
8. Analyze recent high-profile enforcement actions to extract critical lessons in governance failure.
9. Implement technical and organizational measures (TOMS) to demonstrate accountability and mitigate regulatory fines.
10. Navigate the complexities of third-party risk and managing breaches originating from supply chain vulnerabilities.
11. Practice the essential steps of containment, eradication, and recovery for common attack vectors like Ransomware and Cloud Misconfiguration.
12. Conduct effective Post-Incident Reviews to drive continuous improvement in cyber hygiene and the DBIRP.
13. Integrate breach management with wider organizational frameworks, including Data Protection Impact Assessments and DSAR Management.

Target Audience Segments

1. Data Protection Officers and Privacy Managers.
2. Compliance and Legal Professionals
3. IT Security and Incident Response Team members
4. Audit and Governance Professionals.
5. C-Suite Executives.

6. HR and Marketing/PR Managers.
7. Vendor and Third-Party Risk Managers.
8. Consultants and Auditors specializing in Cyber Risk and Regulatory Compliance.

Course Modules

Module 1: The Global Regulatory Landscape & Legal Threshold

- Defining a Personal Data Breach across multiple jurisdictions.
- Trigger events and the importance of reasonable suspicion in commencing an internal investigation.
- The Territorial Scope challenge.
- Distinguishing between mandatory Regulator Notification and Data Subject Notification thresholds.
- Case Study: Change Healthcare Ransomware Attack.

Module 2: Triage, Containment, and the 72-Hour Clock

- The Golden Hour of incident response.
- Executing the first three phases of the DBIRP
- Establishing a secure, privileged Communication Channel for the response team.
- Crucial information gathering for the initial 72-hour regulator notification
- Case Study: AT&T Data Breach.

Module 3: Digital Forensics and Evidence Preservation

- Techniques for maintaining the Chain of Custody and the legal admissibility of evidence.
- Identifying and securing critical data sources.
- The role of the Data Protection Officer in overseeing forensic activities and ensuring compliance.
- Balancing business continuity requirements with the need for immediate system shutdown and forensic imaging.
- Case Study: MOVEit Transfer Vulnerability

Module 4: Risk Assessment and Impact Analysis (DPIA/PIA)

- Conducting a swift Risk to Rights and Freedoms assessment to determine notification necessity.
- Quantifying the potential severity and likelihood of harm.
- The process for documenting the mitigating actions taken prior to and during the breach.
- The role of the Data Mapping/Inventory in rapidly identifying affected data subjects and records.
- Case Study: National Public Data Leak.

Module 5: Regulator and Data Subject Notification

- Structuring a compliant notification to the Supervisory Authority with all required details.
- Drafting the Data Subject Notification to be clear, transparent, and actionable
- Managing exceptions to notification
- Handling cross-border breach reporting and the process of the Lead Supervisory Authority under GDPR.
- Case Study: Ticketmaster/Live Nation Breach.

Module 6: Remediation and Post-Breach Financial Impact

- Implementing Eradication and definitive system hardening measures to prevent re-entry.
- Managing post-breach obligations.
- Understanding the factors that influence regulatory fine calculation

- Insurance requirements.
- Case Study: Colonial Pipeline Ransomware.

Module 7: Supply Chain and Third-Party Breach Management

- Defining roles and responsibilities between Controller and Processor in the event of a breach.
- Contractual obligations and the importance of timely breach notification clauses in vendor agreements.
- Assessing vendor cyber-hygiene and incident response maturity before a breach.
- Strategies for effectively managing a breach that originated in a cloud service provider or SaaS tool.
- Case Study: Snowflake Cloud Attacks.

Module 8: Audit, Review, and Continuous Improvement

- Conducting a formal Post-Incident Review to assess the effectiveness of the DBIRP and team performance.
- Implementing Lessons Learned and prioritizing necessary updates to the DBIRP, policies, and technical controls.
- Using breach data to inform and update the Data Protection Impact Assessment and risk register.
- Designing an effective, engaging Security Awareness Training program based on the breach cause.
- Case Study: MGM Resorts Social Engineering Attack.

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