Differential Privacy and Anonymization 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 Big Data and Artificial Intelligence (AI) has created unprecedented capabilities for data-driven decision-making, yet it has simultaneously amplified privacy risk and data breaches. Traditional anonymization techniques, such as k-anonymity and pseudonymization, are increasingly vulnerable to sophisticated re-identification attacks through data linkage. Organizations face a critical imperative to meet stringent global data privacy regulations like GDPR, CCPA, and emerging AI-specific laws. This context demands the adoption of mathematically rigorous methods that provide provable privacy guarantees without severely compromising data utility for analytics and Machine Learning (ML) model training.

Differential Privacy and Anonymization Training Course offers a deep dive into the privacy-preserving technologies (PETs) and anonymization techniques essential for the modern data ecosystem. Participants will master the theoretical foundations, practical implementation, and real-world trade-offs of DP, moving beyond compliance-based checkboxes to build a proactive Privacy by Design culture. The curriculum emphasizes practical application using leading DP frameworks and Python libraries, covering everything from core mechanisms like the Laplace Mechanism to advanced topics like Federated Learning and Private Machine Learning. Equip your team with the future-proof skills needed to unlock the value of sensitive data while ensuring robust algorithmic fairness and data governance.

Programme Curriculum

Differential Privacy and Anonymization Training Course

Introduction

The proliferation of Big Data and Artificial Intelligence (AI) has created unprecedented capabilities for data-driven decision-making, yet it has simultaneously amplified privacy risk and data breaches. Traditional anonymization techniques, such as k-anonymity and pseudonymization, are increasingly vulnerable to

sophisticated re-identification attacks through data linkage. Organizations face a critical imperative to meet stringent global data privacy regulations like GDPR, CCPA, and emerging AI-specific laws. This context demands the adoption of mathematically rigorous methods that provide provable privacy guarantees without severely compromising data utility for analytics and Machine Learning (ML) model training.

Differential Privacy and Anonymization Training Course offers a deep dive into the privacy-preserving technologies (PETs) and anonymization techniques essential for the modern data ecosystem. Participants will master the theoretical foundations, practical implementation, and real-world trade-offs of DP, moving beyond compliance-based checkboxes to build a proactive Privacy by Design culture. The curriculum emphasizes practical application using leading DP frameworks and Python libraries, covering everything from core mechanisms like the Laplace Mechanism to advanced topics like Federated Learning and Private Machine Learning. Equip your team with the future-proof skills needed to unlock the value of sensitive data while ensuring robust algorithmic fairness and data governance.

Course Duration

5 days

Course Objectives

1. Master the mathematical foundation of Differential Privacy
2. Evaluate the limitations of traditional Anonymization Techniques
3. Implement the Laplace Mechanism and Exponential Mechanism for query release.
4. Analyze the Privacy-Utility Trade-off in real-world data releases.
5. Apply Differential Privacy in SQL Databases for generating private aggregates.
6. Develop and train Differentially Private Machine Learning models.
7. Integrate Federated Learning with Differential Privacy for decentralized training.
8. Understand the principles of Privacy by Design and Data Minimization.
9. Assess and manage Privacy Budget allocation across multiple analyses.
10. Explore Local Differential Privacy applications in consumer data collection.
11. Interpret the practical implications of DP in various Regulatory Compliance contexts.
12. Mitigate risks associated with Data Leakage and Re-Identification Attacks.
13. Utilize open-source DP Frameworks.

Target Audience

1. Data Scientists & ML Engineers.
2. Data Engineers & Architects.
3. Chief Privacy Officers (CPOs) / Data Protection Officers
4. Security Analysts & Engineers.
5. Compliance & Legal Professionals.
6. Product Managers
7. Quantitative Researchers & Statisticians.
8. Cloud & Software Engineers.

Course Modules

Module 1: Foundational Concepts in Data Privacy

- Definition of Personal Data and PII.
- The spectrum of Anonymization techniques

- Understanding the risks: Linkage Attacks and auxiliary information.
- Introduction to Differential Privacy.
- The fundamental Privacy-Utility Trade-off.
- Case Study: Netflix Prize Re-identification.

Module 2: The Mathematics of Differential Privacy

- Formal definition of $(\epsilon, \delta) $-Differential Privacy.
- Understanding the role of the Privacy Budget (ϵ) and its implication for risk.
- Case Study: Concepts of Sensitivity.
- The power of Post-Processing Immunity.
- Composition of DP mechanisms.

Module 3: Implementing Core Differential Privacy Mechanisms

- In-depth study and Python implementation of the Laplace Mechanism for numeric queries.
- Application of the Exponential Mechanism for non-numeric and selection queries.
- Clipping as a prerequisite for noise addition.
- Handling count and boolean queries with the Geometric Mechanism.
- Practical hands-on lab using a DP library.
- Case Study: Private Aggregates in US Census Data.

Module 4: Differential Privacy in SQL and Data Analytics

- Implementing DP on tabular data using private **SQL** queries.
- **Data Aggregation** with differential privacy
- Techniques for private query optimization and performance.
- Case Study: The challenge of **Sparse Data** and managing small groups.
- Release of differentially private **Synthetic Data**.

Module 5: Differential Privacy in Machine Learning

- Introduction to Private Machine Learning and its necessity.
- Differentially Private Stochastic Gradient Descent for model training.
- The concept of Model Inversion Attacks and how DP mitigates them.
- Analysis of the impact of DP on Model Accuracy.
- Tools and frameworks for DPML.
- Case Study: Google's DP-SGD in Production.

Module 6: Federated Learning and Local Differential Privacy

- Architecture and benefits of Federated Learning
- FL with DP.
- Understanding Local Differential Privacy.
- LDP mechanisms for user-level data collection.
- Use cases for LDP in telemetry and analytics.
- Case Study: Apple's Use of Local Differential Privacy.

Module 7: Privacy Budget Management and Auditing

- Strategic allocation and decay of the Privacy Budget.
- Methods for Privacy Loss Accounting across sequential queries.

- Understanding the challenge of Adaptive Attacks.
- Tools for DP Auditing and compliance verification.
- Case Study: Best practices for developing a robust DP Policy framework.

Module 8: Advanced DP Topics and Regulatory Landscape

- Advanced mechanisms
- The convergence of DP with other PETs.
- Navigating the regulatory requirements.
- Ethical implications: Algorithmic Fairness and bias in DP data.
- Future trends in Privacy Enhancing Technologies
- Case Study: Uber's Use of DP for Geospatial Data.

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