DATA/>rotocol

PRIVACY ENGINEERING CERTIFICATION

Nishant Bhajaria, Executive Producer & Lead Instructor

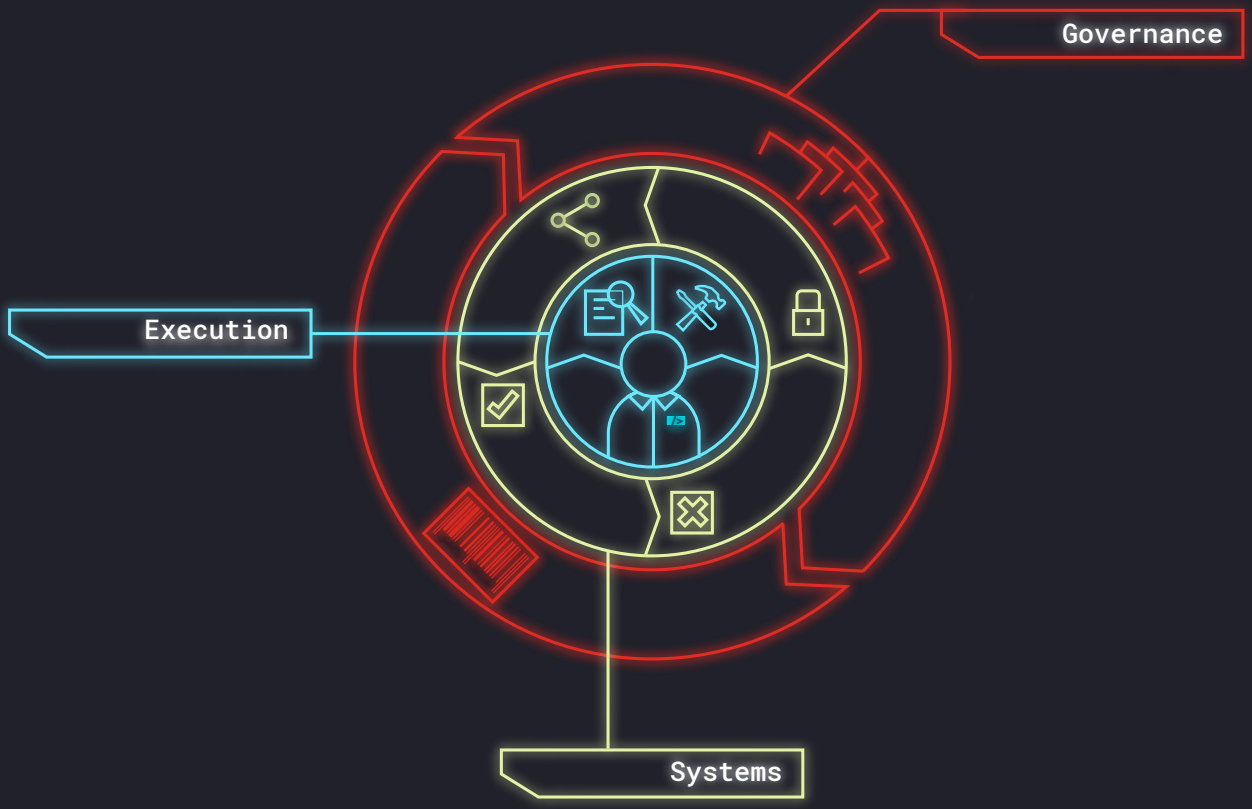
Kimber Bougan, VP of Learning - Data Protocol

Data Protocol's Privacy Engineering program provides engineers the foundational skills to build privacy and data security into their products and processes. The curriculum for this certification program teaches and tests developers' ability to design secure data processes and address pre-existing vulnerabilities.

Led by visionary privacy technologist Nishant Bhajaria, Data Protocol's Privacy Engineering certification validates design skills, technical knowledge, and topical proficiency. The eight course certification program and hands-on labs lay the foundation for effective data management and provide valuable situational experience. The future will increasingly value data management and privacy with each year and each innovation. Privacy engineers are rising to meet the challenge.

The final assessment and subsequent administration of the Privacy Engineering verification by Data Protocol costs $495.

Program Overview



Governance

Data Classification

Data Categorization

Execution

Privacy Tech

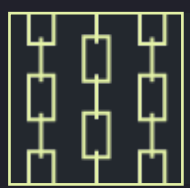
Beyond Privacy Review - Technical Privacy Consulting

Systems

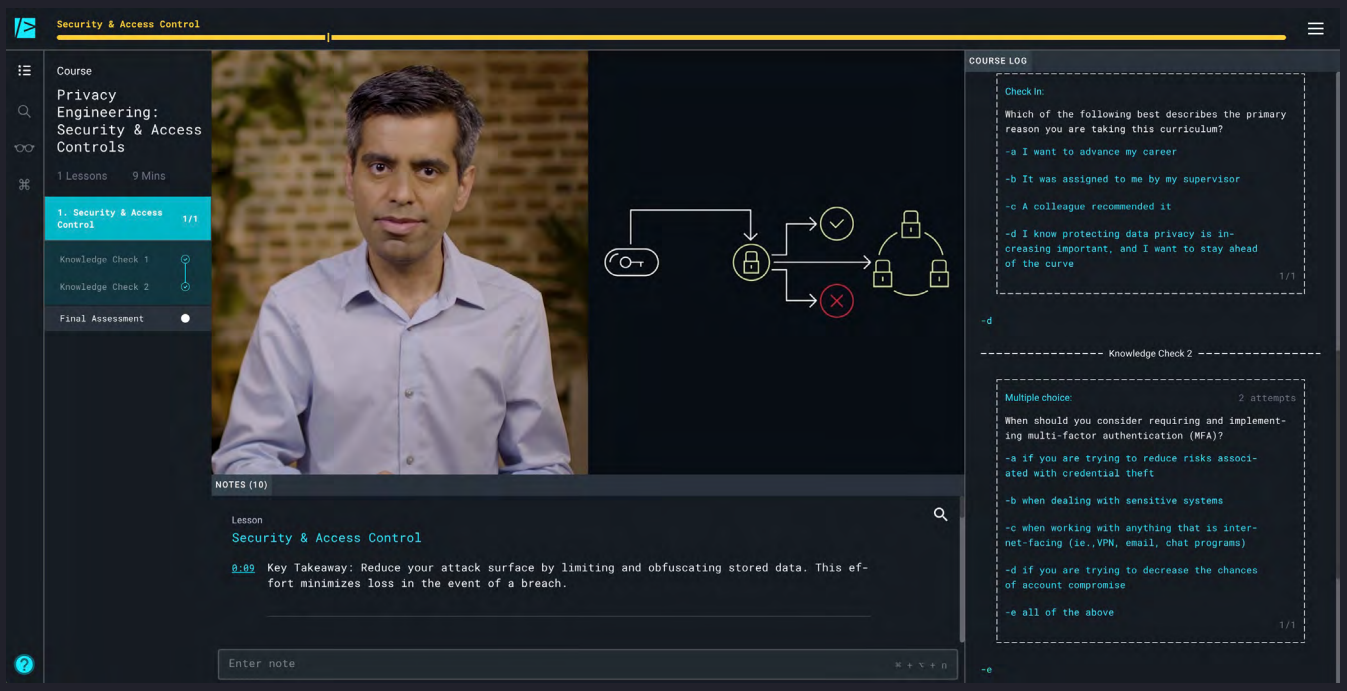
Data Sharing

Consent Management

Data Deletion



Security & Privacy



Learner Profile

While anyone working in the tech space will benefit from this curriculum, the Privacy Engineering Certification curriculum is primarily designed for developers with:

- 2-3 years of experience as a full-stack developer building and deploying either centralized services (one to many) or smaller services that are managed by a centralized service (many to one)
- an understanding of the data flow from an edge API to a data warehouse
- an appreciation for the scale of modern infrastructure
- knowledge of current policy and regulatory environments surrounding data privacy (e.g., GDPR, CCPA). To familiarize yourself with these topics, you can learn more through the following courses available on the Data Protocol platform:
    - Data Regulations for Developers
    - TLDR; GDPR

Certification Overview

(6-8 Hours)

Intro to Privacy Engineering (est. time: 10 min)

- Privacy Engineering Introduction
- Understanding Data Flow

Governance Module (est. time: 130)

Data Classification + Lab (Data Classification)	Why Data Governance Matters Data Classification: Process Data Classification in Practice Privacy Control Models Privacy Control in Practice Conclusion
Data Categorization + Lab (Data Inventory) + Lab (Retrievability)	Introduction Data Tagging Data Inventory System Structuring Metadata Measuring Success
Data Governance Conclusion	

Systems Module (est. time: 140 min)

Systems Introduction	
Consent Management + Lab (Consent Management)	Introduction Overview Consent Management Platform Conclusion
Security & Privacy	Introduction Attack Surface Enterprise Risk Model Security & Access Controls Access Control Gaps Conclusion

Data Deletion + Lab (Data Deletion)	Introduction Why Deletion is Important Data Collection Architecture Tooling & Processes Automation & Scaling Conclusion
Data Sharing + Lab (K-Anonymity and L-Diversity)	Introduction Sharing Data Safely Data Anonymization Measuring Impact Conclusion
Systems Conclusion	

Execution Module (est. time: 40 min)	
Execution Introduction	
Privacy Tech	Introduction Build vs Buy Tooling Overview Risks
Beyond Privacy Review - Technical Privacy Consulting	Introduction Privacy Reviews Overview Process Documentation Use Cases Conclusion
Conclusion	

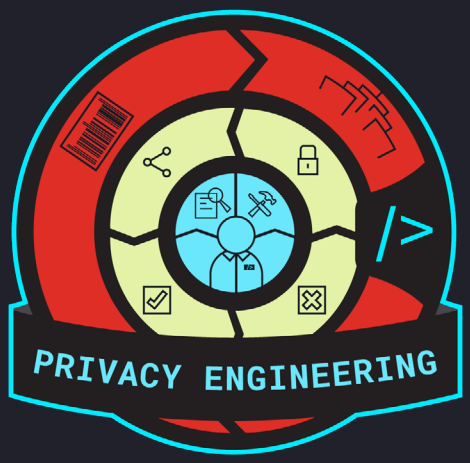
CURRICULUM & COURSE DESCRIPTIONS

Privacy Engineering Certification Description

Data Protocol's Privacy Engineering curriculum provides engineers and technical professionals the foundational skills to build privacy and data security into their products and processes. Each of the eight courses comprising this program teaches and tests your ability to design secure data processes and address pre-existing vulnerabilities. Hands on labs will provide situational experience and validate your privacy engineering and design skills. Upon the completion of the curriculum, passage of a comprehensive final assessment will validate and certify your proficiency.

Each course can stand alone, but you must complete the full curriculum to be eligible for certification.

Program



The privacy engineering curriculum is structured in three modules: governance, systems, and execution.

Governance: Technical implementation of processes and policies to manage the data a company collects and provides the ability to measure the risk that the data poses to the business.

Systems: We cover the four critical point-solutions you'll need to put in place for any privacy engineering program: sharing, consent, deletion, and security. Instead of frantically searching for tools to address a privacy incident when one occurs, you'll thoughtfully select and implement these systems to prevent privacy incidents from occurring in the first place.

Execution: Provides real-world guidance on how to implement a privacy engineering program that faces build vs buy considerations on tooling and how to help engineers align with legal teams to avoid the last minute "ship or block" conversation.

Why Is This Program Structured This Way?

For most companies, privacy only becomes a priority after an incident has occurred. When this happens, there's an urgency to find a solution to fix that incident without doing the necessary work to prevent it from occurring again. This program is designed to teach developers how to create sound data governance that provides a solid foundation to inform privacy controls.

Governance Module

Data Classification

Course: Data classification is the foundation of privacy engineering. If you can't identify and measure the risk profile of your data, you can't manage its value, its flow, or its security. This course will teach you how to classify and map data throughout your systems according to its risk level, retention requirements, and access policies.

Hands on Lab: Learners will classify data, transform the dataset based on that classification, and consider how the risk to privacy should impact storage and access.

Data Categorization

Course: With a strong foundation of data categorization in place, this course will teach you the techniques to optimize data flow in support of privacy and business operations. Specifically, you will learn about tagging data, building a system architecture to discover data, and measuring the success of your categorization program. These techniques will enable you to identify all of your data and automate privacy.

Hands on Lab: Learners will complete two lab exercises for Data Categorization. First, they will crawl a dataset to understand overall privacy risk, introduce a new data pipeline by creating different datasets, and make decisions about access control and retention.

Then, learners will complete a Data Retrieval lab. In this exercise, they will use modeling to demonstrate the impact of poor data hygiene and governance on the time required to retrieve data when needed, like in response to a DSAR.

Systems Module (est. 140 min)

Data Sharing

Course: Data is most at risk when it is in motion, but data sharing is a necessity to support customer engagement, business continuity, and product innovation. Effective privacy engineering eliminates the need to choose between the two. In this course, you will learn to prioritize data minimization, anonymization, and channel segmentation to protect data in motion while ensuring it is available when and how it is needed. Finally, you will learn how to quantify the impact of your efforts to manage privacy risk.

Hands on Lab: Learners will coarsen a dataset, measure the impact of their efforts using K-Anonymity, and consider how L-Diversity can be applied to further protect data privacy.

Consent Management

Course: Data management should start at the source. Implementing an effective consent management system is critical to protecting and operationalizing data. In this course, you will learn the proper way to secure and maintain informed and granular consent in compliance with data regulations, and to promote user trust. You will learn how to implement a flexible Consent Management Platform and manage the common complexities created by multiple variables such as features, locations, and version control.

Hands on Lab: Learners will evaluate a consent management backend to understand how a complex platform will impact data management processes like retrieval, storage, and deletion.

Data Deletion

Course: Data deletion is critical to regulatory compliance and overall privacy protection. Effective data classification and categorization enable data deletion upon request or once it is no longer required. In this course, you will learn about implementing, automating, and scaling deletion in a distributed environment. This includes the basics of deletion, how designing a process for deletion relies on understanding the data collection architecture, and the tools and processes you will use from implementation to scaling.

Hands on Lab: Learners will use a deletion service to find a test user, confirm that user can be legally deleted from the database, delete the user, and confirm that the deletion was successful.

Security & Privacy

Course: A privacy engineer does not need to be a security expert, but you do need to understand how to manage and use data securely. In this course, you will learn how to build a framework that reduces the attack surface for sensitive data and how to implement tools for the management of access control and monitoring, such as Access Control Lists (ACLs) and encryption keys.

Execution Module (est. 40 min)

Privacy Tech

Course: The importance of data privacy and the rise of privacy engineering has driven innovation and availability of privacy technologies. As a privacy engineer, you have options. Determining what tools to use for your specific needs is an important part of the job. In this course, you will begin to consider what tools you need to execute your plan, and why. Specifically, you will learn some of the key players in the privacy tooling space, the criteria you should use when shopping for solutions, and the pros and cons of building versus buying.

Beyond Privacy Review - Technical Privacy Consulting

Course: You have learned how - and why - privacy should be designed into your systems, your processes, and your products. As a privacy engineer, you work to limit risk as early as possible with both a strategic plan and the right tools. It is also your job to maintain the program you've designed and built by continually assessing risks and protections. In this course, you will learn a new approach to the traditional privacy review, a process that often occurs too late. Implementing ongoing technical privacy consulting through out your existing program will reduce risks and avoid costly mitigations.