Module 9

Kickoff Workshop

Icebreaker

Which Is the Better Data Decision?

Below are 4 data-related actions. Can you guess which ones help protect ML systems and which ones could put data at risk?

1. Share login credentials with your team for quick access
2. Use encryption when storing training data
3. Download sensitive data sets onto a personal USB drive
4. Limit access to ML systems using role-based permissions

Module 9

Kickoff Workshop

Agenda

- Welcome and introduction
- Module overview
- Applying module skills
- Project overview
- Q&A
- Next steps

Module overview

Your learning journey

Week 1	Kickoff Workshop	Async Unit 1	Live Workshop 1
Week 2	Async Unit 2	Async Unit 3	Live Workshop 2
Week 3	Wrap-Up Workshop	Project tasks	
Week 4	Group Coaching		

Module skills: from learning to applying

Understand security principles specific to ML workflows	Implement safeguards that protect data and models throughout the ML lifecycle by applying principles like encryption, access control, and audit trails to reduce risk of breach or tampering.
Design and implement compliant ML systems	Build ML pipelines that align with GDPR or other data privacy regulations by integrating consent mechanisms, data minimisation, and transparent data handling policies.
Develop strategies to identify, assess, and mitigate ML compliance and privacy risks	Use risk assessment frameworks like DPIAs (Data Protection Impact Assessments) to proactively flag and reduce privacy or ethical issues in ML deployment environments.

Skill 1 in the real-world

Design and implement compliant ML systems

In 2021, Meta implemented a system-wide update to its ad-targeting ML pipeline to comply with new EU privacy regulations, restructuring its model training workflows to exclude sensitive personal data fields.

This helped Meta avoid regulatory fines, maintain platform trust, and continue providing personalised experiences without breaching GDPR rules.

By automating compliance checks across ML workflows, teams can proactively adapt to future regulations and reduce the risk of costly rework or penalties.

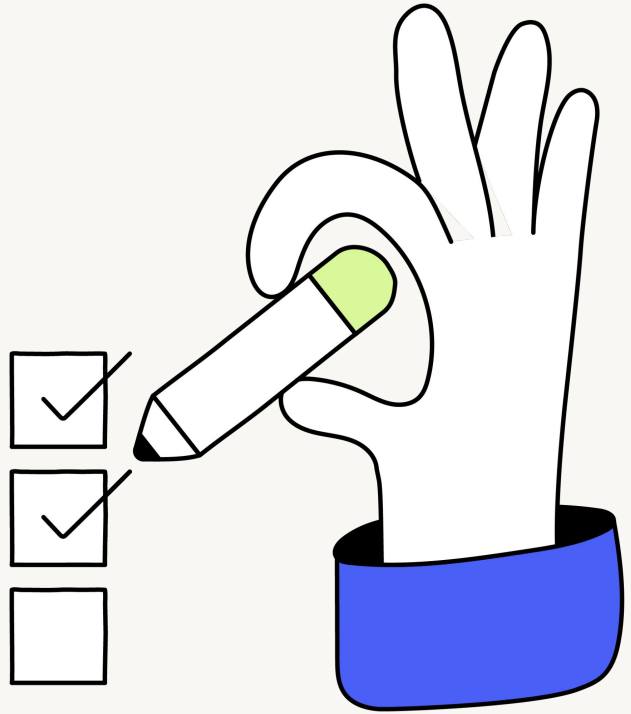
Applying module skills to your workplace

Skills application brainstorm

Choose a module skill and think of 3 ways to apply it in your role

Create a post for the group explaining how you'd like to apply this skill this month

Post your explanation in the Skill Application Brainstorm discussion board



Skill application share out

1. Review other discussion posts.
2. Choose another person’s post that you think is a great example of applying the skill.
3. Raise your hand to share your thoughts.

Project overview

Phase 2 project: Applying ML techniques

Project objective: Build and refine an ML model for performance, fairness, and security. Use XAI to address bias, define key metrics, and ensure full compliance with robust documentation and retraining plans.

Module 6 milestone: Model Engineering and Training

Module 7 milestone: Optimising Models

Module 8 milestone: Model Evaluation

Module 9 milestone: Data Security, Privacy, and Governance

We are here!

Module 9 milestone: Applying ML techniques

Phase project objective: Build and refine an ML model for performance, fairness, and security. Use XAI to address bias, define key metrics, and ensure full compliance with robust documentation and retraining plans.

Milestone task 1

Security fundamentals in machine learning: Assess cybersecurity risks related to the ML model, including data access controls, adversarial attacks, and security vulnerabilities.

Milestone task 2

Data privacy and governance in machine learning: Apply organisational policies and industry frameworks (e.g., AREA, SAFE-D) to ensure compliance with data privacy and governance regulations.

Milestone task 3

Regulatory compliance and risk management in machine learning Conduct an audit to verify compliance with legal, ethical, and governance requirements. Document the full lifecycle of the ML model from development to deployment.

Module 9 milestone: KSB requirements

Phase project objective: Build and refine an ML model for performance, fairness, and security. Use XAI to address bias, define key metrics, and ensure full compliance with robust documentation and retraining plans.

Task 1 KSBs	**Security fundamentals in machine learning:** K27
Task 2 KSBs	**Data privacy and governance in machine learning:** K25, S11, S32
Task 3 KSBs	**Regulatory compliance and risk management in machine learning:** S6, S17, S32

Questions?

Closing out

- **Action items:** Async Unit 1
- **Have questions?**
  - Chat with Atlas
  - Reach out to your Cohort Coach
  - Sign up for Tutoring
- **Log your OTJ hours**
- **Take the Workshop Survey** on My Multiverse

multiverse