AI Literacy: Technical Foundations for Non-Tech Roles

This course is part of the **AI Literacy** series and is designed to help meet the *AI literacy requirements* set out in **Article 4** of the **EU AI Act**, which entered into force on 2 February 2025.

By building the skills, knowledge, and understanding to interact effectively and responsibly with AI systems, you will not only improve your day-to-day results but also strengthen your organisation's compliance posture. The courses focus on practical, plain-language learning that benefits any role, from operational staff to senior leadership, while ensuring you can oversee, apply, and guide AI use with competence, compliance, and confidence.

PRIMER: UNDERSTANDING CHATGPT IN ENTERPRISE & PUBLIC CONTEXTS

+94767033426 250, Liberty Plaza, Colombo 03 librasentinel.lk@gmail.com

AI Literacy: Technical Foundations for Non-Tech Roles

MODULE 1: THE TECHNICAL CORE WITHOUT THE JARGON

1.1 What's Under the Hood: Inputs, Models, Outputs

1.1.1 How AI turns prompts into outputs
1.1.2 The role of model architecture in shaping responses
1.1.3 Why understanding this flow helps you work with AI effectively

1.2 How Machines "Learn" from Data (Training vs. Fine-tuning)

1.2.1 Large-scale training on diverse datasets
1.2.2 Fine-tuning for specific industries or tasks
1.2.3 How training choices affect accuracy and bias

1.3 Parameters, Tokens, and Context Windows – Why They Matter

1.3.1 Parameters as the model's learned settings
1.3.2 Tokens as the units of information AI processes
1.3.3 Context window limits and their impact on long documents

1.4 Model Limitations and "Boundaries of Competence"

1.4.1 Lack of live internet access unless enabled
1.4.2 Outdated training data and its consequences
1.4.3 Recognising when the model is outside its reliable scope

MODULE 2: TYPES OF AI SYSTEMS YOU WILL ENCOUNTER AT WORK

2.1 LLMs vs. Traditional AI Models

2.1.1 Large Language Models (LLMs) for natural language tasks
2.1.2 Traditional AI for structured, specialised tasks
2.1.3 Why knowing the difference matters for risk and compliance

2.2 OpenAI, Azure OpenAI, Anthropic, and Proprietary In-House Models

2.2.1 Public platforms accessible to anyone
2.2.2 Enterprise versions with enhanced controls
2.2.3 Fully in-house models built for maximum data control

2.3 Embedded AI in Tools You Already Use

2.3.1 AI features inside office software and business apps
2.3.2 How "hidden" AI can affect compliance
2.3.3 Spotting AI-driven outputs in everyday workflows

+94767033426
250, Liberty Plaza, Colombo 03
librasentinel.lk@gmail.com

2.4 AI as a Service (APIs, Integrations, Connectors)

2.4.1 APIs for custom AI-powered features
2.4.2 Pre-built integrations in workplace tools
2.4.3 Data flow considerations when systems connect to AI

MODULE 3: DATA FLOWS AND PRIVACY IMPLICATIONS

3.1 Where Your Data Goes (On-device, Cloud, Third-party)

3.1.1 How on-device AI processes data locally
3.1.2 Cloud-hosted AI and remote data processing
3.1.3 Third-party services involved in AI workflows

3.2 Data Retention, Sharing, and Training Policies

3.2.1 How long vendors store your data
3.2.2 Who your data may be shared with
3.2.3 Whether your data is used to train the AI

3.3 Privacy by Design and Data Minimisation in AI

3.3.1 Embedding privacy protections into AI tools
3.3.2 Sharing only what's necessary for the task
3.3.3 Practical examples of data minimisation

3.4 Identifying and Managing Regulated Data Inputs (PII, Health, Finance)

3.4.1 Recognising personal and sensitive data
3.4.2 Understanding legal and regulatory boundaries
3.4.3 Preventing prohibited data from entering AI systems

MODULE 4 - AI RISKS: ACCURACY, BIAS, AND SECURITY

4.1 Accuracy Errors and "Hallucinations" in Context

4.1.1 How AI produces wrong or incomplete information
4.1.2 Why hallucinations happen even in advanced models
4.1.3 Examples of hallucinations in workplace settings

4.2 Bias in Models: How It Happens and Why It Matters

4.2.1 Bias from training data and historical patterns
4.2.2 Discrimination risks in hiring, lending, and other areas
4.2.3 Vendor approaches to bias detection and mitigation

4.3 Security Vulnerabilities in AI Workflows

4.3.1 Prompt injection attacks and manipulation risks
4.3.2 Data leakage from AI responses
4.3.3 Risks from plugins, connectors, and integrations

+94767033426
250, Liberty Plaza, Colombo 03
librasentinel.lk@gmail.com

4.4 Mapping Risks to Controls (Human Oversight, Testing, Red Teaming)

4.4.1 Keeping humans in decision loops
4.4.2 Testing AI systems before deployment
4.4.3 Simulating misuse to find vulnerabilities

MODULE 5: AI IN THE ENTERPRISE ENVIRONMENT

5.1 Public vs. Enterprise AI Platforms

5.1.1 Public AI accessible to anyone
5.1.2 Enterprise AI with enhanced security and controls
5.1.3 Why platform choice impacts compliance and risk

5.2 On-Premises, Cloud, and Hybrid Deployments

5.2.1 On-premises AI for maximum control
5.2.2 Cloud AI for scalability and vendor support
5.2.3 Hybrid setups for balancing security and flexibility

5.3 AI Access Controls and User Management

5.3.1 Role-based permissions for AI tools
5.3.2 Monitoring and audit logging of AI use
5.3.3 Managing access for compliance and security

5.4 Vendor Management and SLAs for AI Services

5.4.1 Evaluating AI vendors for compliance readiness
5.4.2 Key terms to look for in AI service contracts
5.4.3 Holding vendors accountable for performance and security

MODULE 6: SPEAKING "TECH" TO TECHNICAL TEAMS

6.1 Translating Business Needs into Technical Requirements

6.1.1 Defining the goal before the solution
6.1.2 Describing processes and expected outputs clearly
6.1.3 Avoiding assumptions about technical design

6.2 Reading and Interpreting AI System Documentation

6.2.1 Identifying input requirements
6.2.2 Understanding outputs and constraints
6.2.3 Using documentation to check system suitability

6.3 Asking the Right Questions in AI Project Meetings

6.3.1 Probing for data handling details
6.3.2 Clarifying how the system handles edge cases
6.3.3 Confirming bias and accuracy testing steps

6.4 Common Misunderstandings Between Business and Tech Roles

6.4.1 Business-side assumptions that cause issues
6.4.2 Technical miscommunications with non-tech teams
6.4.3 Bridging gaps with plain-language recaps

MODULE 7: FROM KNOWLEDGE TO ACTION

7.1 Mapping AI Capabilities to Your Role

7.1.1 Listing your core tasks and workflows
7.1.2 Matching tasks to suitable AI capabilities
7.1.3 Evaluating AI fit based on accuracy and risk

7.2 Designing AI-Ready Processes Without Over-automation

7.2.1 Identifying safe automation opportunities
7.2.2 Keeping humans in decision-critical steps
7.2.3 Balancing efficiency with governance needs

7.3 Creating an AI Usage Risk Checklist for Your Team

7.3.1 Checking for sensitive or regulated data
7.3.2 Including accuracy and bias verification steps
7.3.3 Documenting AI-assisted decisions for accountability

7.4 Continuous AI Literacy: Staying Current in a Fast-Moving Field

7.4.1 Following organisational AI updates
7.4.2 Tracking regulatory changes
7.4.3 Refreshing skills through periodic training

MODULE 8: GPT-5 AGENTIC CONTROLS & TOOLS

8.1 Understanding Agentic Behaviour

8.1.1 What agentic means in GPT-5
8.1.2 Planning and tool use without constant instructions
8.1.3 When to allow vs limit autonomy

8.2 The Autonomy Dial – Eagerness Settings

8.2.1 Low vs high eagerness modes
8.2.2 Matching autonomy level to task risk
8.2.3 Productivity vs oversight trade-offs

8.3 Tool Preambles for Transparency

8.3.1 What tool preambles are
8.3.2 How they show AI reasoning before action
8.3.3 Using preambles to improve trust

8.4 Output Control – Verbosity & Reasoning Effort

8.4.1 Controlling length separately from depth
8.4.2 Allocating reasoning effort for complex work
8.4.3 Combining settings for best results

This course is part of the ***AI Literacy series*** - a connected set of courses designed to give professionals at every level the skills, knowledge, and confidence to work effectively and responsibly with AI.

Where ***AI Literacy – Technical Foundations for Non-Tech Roles*** builds your essential technical understanding, the series continues with focused courses like ***AI Literacy: Understanding LLMs*** and ***AI Literacy: Prompt Fluency Toolkit***, each building on the last so your AI skills grow in depth and sophistication.