

DAY 1 – BASIC LEVEL

Theme: Cyber Awareness, Digital Safety & GDPR Foundations

2. Digital Transformation in the Tourism Ecosystem
 - 2.1 Digitalisation Trends in EU Tourism and Hospitality
 - 2.2 Regulatory Expectations in a Digital Tourism Environment
 - 2.3 Why Cybersecurity and Data Protection Matter in Tourism
 - 2.4 Employee Roles in Protecting Guests, Data, and Brand Trust
 3. Understanding Cyber Threats in Tourism
 - 3.1 Overview of Common Cyber Threats
 - 3.2 Phishing, Social Engineering, and Email Scams
 - 3.3 Fake Bookings, Payment Fraud, and Online Scams
 - 3.4 Malware and Ransomware Attacks
 - 3.5 Threats Targeting Front Desk Systems, Booking Platforms, and Mobile Devices
 - 3.6 Real-World EU and Global Tourism Cyber Incident Scenarios
 4. Safe Online Behaviour and Cyber Hygiene
 - 4.1 Password Security and Authentication Best Practices
 - 4.2 Use of Password Managers and Multi-Factor Authentication
 - 4.3 Secure Use of Public Wi-Fi and Remote Work Practices
 - 4.4 Device Security for Laptops, Mobiles, and Tablets
 - 4.5 Identifying Suspicious Links, Attachments, and QR Codes
 5. GDPR Fundamentals and Data Privacy Awareness
 - 5.1 Introduction to GDPR and EU Data Protection Principles
 - 5.2 Personal Data vs. Special Category Data in Tourism
 - 5.3 Lawful Bases for Processing Guest Data
 - 5.4 Data Minimisation, Purpose Limitation, and Retention
 - 5.5 Do's and Don'ts When Handling Guest IDs, Passports, and Payment Information
 - 5.6 Employee Responsibilities in Preventing Data Breaches
 6. Secure Digital Communication and Online Presence
 - 6.1 Safe Use of Email and Messaging Platforms
 - 6.2 Social Media Risks and Oversharing
 - 6.3 Impersonation, Fake Reviews, and Online Reputation Threats
 - 6.4 Maintaining Brand Trust and Digital Professionalism
 7. Day 1 Knowledge Check and Review
 - 7.1 Interactive Quiz and Scenario-Based Questions
 - 7.2 Key GDPR and Cyber Hygiene Takeaways
 - 7.3 Behavioural Checklist for Daily Operations
-

DAY 2 – ADVANCED LEVEL

Theme: Secure Practices, Compliance & Future-Ready Workforce

8. Advanced Cybersecurity Concepts for Non-Technical Staff
 - 8.1 How Cyber Attacks Happen: Simplified Attack Lifecycle
 - 8.2 Human Error, Insider Threats, and Social Engineering
 - 8.3 Business Email Compromise (BEC) and Financial Fraud
 - 8.4 Secure Use of Cloud-Based Tourism Systems
9. Secure Use of Digital Tools and Third-Party Platforms
 - 9.1 Security Considerations for Reservation and Booking Systems
 - 9.2 CRM Tools and Guest Data Protection
 - 9.3 Online Payment Gateways and PCI-DSS Awareness
 - 9.4 Third-Party Vendors, Data Processors, and Shared Responsibility
 - 9.5 GDPR Requirements for Data Sharing and Cross-Border Transfers
10. Incident Awareness, Reporting, and Response
 - 10.1 Identifying a Cybersecurity or Data Protection Incident
 - 10.2 Immediate Actions for Employees (Do's and Don'ts)
 - 10.3 Incident Reporting and Escalation Procedures
 - 10.4 GDPR Breach Notification Requirements (72-Hour Rule)
 - 10.5 Business Continuity and Operational Resilience in Tourism
11. Advanced Digital Competencies and Emerging Technologies
 - 11.1 Secure Use of Digital Collaboration Tools
 - 11.2 Basics of Data-Driven Decision Making
 - 11.3 AI and Automation in Tourism: Opportunities and Risks
 - 11.4 Responsible and Compliant Use of Emerging Technologies
12. Ethics, Trust, and Digital Responsibility
 - 12.1 Ethical Handling of Guest Data and Privacy by Design
 - 12.2 Transparency, Consent, and Guest Rights under GDPR
 - 12.3 Digital Accessibility and Inclusion in the EU Context
 - 12.4 Trust as a Competitive Advantage in Tourism
 - 12.5 Sustainability and Responsible Digital Transformation
13. Final Assessment, Certification, and Action Planning
 - 13.1 Advanced-Level Assessment and Evaluation
 - 13.2 Individual Cyber Safety and GDPR Compliance Action Plan
 - 13.3 Certification of Completion
 - 13.4 Next Steps and Continuous Improvement Roadmap