

EADPP Certification for Data Protection Professionals

Syllabus

Table of Contents

1. Purpose of the Syllabus	2
2. About the EADPP Certification	2
3. About EADPP	3
4. Exam Modalities	4
5. Learning Objectives	4
6. Certificate Content: Privacy Enablers Body of Knowledge and Skills (BOKS).....	5
7. Exam Blueprint	10
8. Exam Preparation.....	11

1. Purpose of the Syllabus

This Syllabus assists candidates in outlining the content of the EADPP Certification for Data Protection Professionals exam. The purpose of this document is to inform candidates about the following:

- EADPP Certification for Data Protection Professionals;
- EADPP's vision and mission;
- Exam modalities;
- Learning objectives;
- Body of Knowledge and Skills (BOKS);
- Exam blueprint; and
- Exam preparation.

For more information on the exam registration process and procedures, and candidate rules and guidelines, please refer to the Candidate Handbook, which is available for download [here](#).

2. About the EADPP Certification

The EADPP Certification is deeply rooted in the European Union (EU)'s robust data protection landscape. The EU has been at the forefront of shaping data protection regulations and standards, with the introduction of the GDPR being a landmark achievement. It is an inclusive Certification, developed and managed by European data professionals, welcoming participation from data protection professionals worldwide. Non-EU professionals and organisations can greatly benefit from the EADPP Certification as it provides them with valuable insights into the EU's data protection culture, enabling them to navigate compliance requirements when dealing with EU personal data processing.

Beyond compliance, the EADPP Certification emphasises the crucial intersection of data protection, privacy, and cybersecurity. There is no privacy without cybersecurity, and a data

protection professional with expertise in both areas is better equipped to develop effective risk management strategies. By understanding and addressing the risks organisations face, such professionals can create policies and procedures that go beyond regulatory compliance to ensure a strong and proactive data protection framework.

A professional with expertise in cybersecurity, policies, and procedures knowing how to create a privacy culture will have a broader range of skills and knowledge than a Data Protection Officer (DPO), who may be more narrowly focused on compliance with data protection regulations. This broader expertise can be valuable in a variety of roles, including consulting, auditing, and policy development. By obtaining this Certificate, the candidate demonstrates a holistic approach to data protection and privacy fundamental cornerstones; including Legislation, Compliance Mechanisms, Information Security, and Work Plan; and acknowledges practical skills on how to make them work in a business environment.

In summary, a data protection professional who successfully completes the EADPP Certification exam, demonstrates their ability to ensure high-quality implementation of data protection measures beyond the legal aspects, ensuring a comprehensive and effective approach to privacy and security.

3. About EADPP

The [European Association of Data Protection Professionals \(EADPP\)](#) is the first independent European non-profit organisation for professionals from around the world who are interested in the General Data Protection Regulation (GDPR) and the protection of personal data. It welcomes any expert in privacy, data, security, and all other relevant areas. EADPP connects these professionals with each other, as well as with other European and international organisations and institutions active in the field of privacy. It serves as a platform for the exchange of opinions, experiences, and knowledge. EADPP aims to provide

its members to confirm or enhance their expertise through the EADPP Certification, developed by Privacy Enablers, and to create a professional network for cooperation.

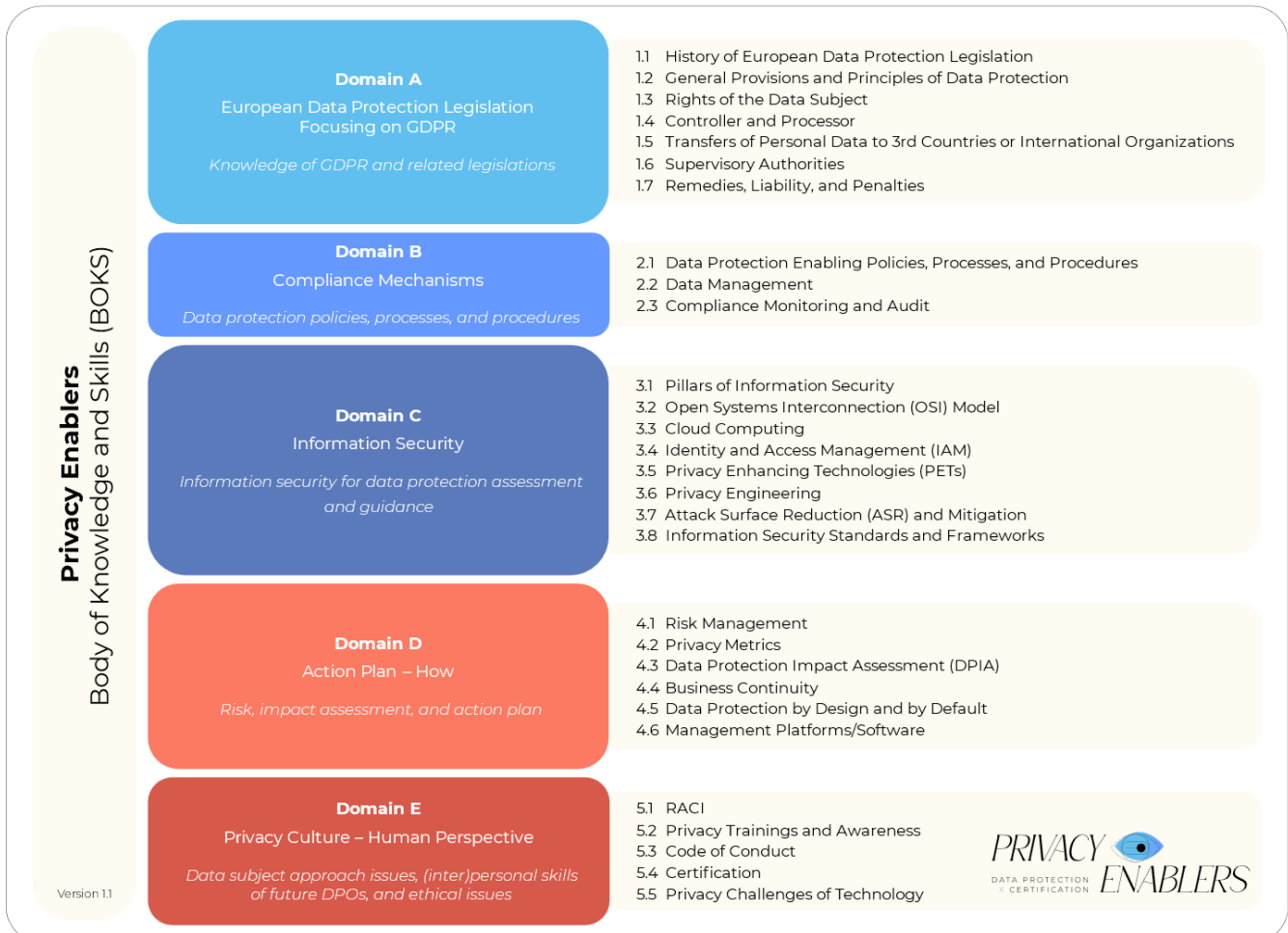
4. Exam Modalities

Type of exam	Single-option questions
Number of questions	40 questions
Exam duration	120 minutes
Passing grade or mark	28/40 (70%)
Method of delivery	Computer-based (online)

5. Learning Objectives

		Domain A: European Data Protection Legislation	Domain B: Compliance Mechanisms	Domain C: Information Security	Domain D: Action Plan	Domain E: Privacy Culture
Learning objectives	Knowledge Remember and understand	<ul style="list-style-type: none"> - Understand the evolution of European data protection legislation - Know GDPR concepts 	<ul style="list-style-type: none"> - Understand the requirements for GDPR compliance - Basic concepts of data governance 	Understand basic principles of information security	<ul style="list-style-type: none"> - Privacy risks - Different data protection frameworks 	Understand building blocks of privacy culture
	Skills Apply	Be able to apply knowledge of legislation to particular situations in business environment	Be able to conduct gap analysis	Implement technical measures and integrate necessary safeguards into the processing	Make contextual analysis	Create awareness programme

6. Certificate Content: Privacy Enablers Body of Knowledge and Skills (BOKS)



© Privacy Enablers

All rights reserved. This document is currently in development, and the information it contains may be subject to change.

Domain	Scope	Sub-domains
<p>Domain A <i>European Data Protection Legislation Focusing on GDPR</i></p>	<p>Knowledge of GDPR and related legislations</p>	<ul style="list-style-type: none"> 1.1 History of European Data Protection Legislation <ul style="list-style-type: none"> 1.1.1 OECD Guidelines 1.1.2 Convention 108 1.2 General Provisions and Principles of Data Protection <ul style="list-style-type: none"> 1.2.1 Material Scope 1.2.2 Territorial Scope <ul style="list-style-type: none"> 1.2.2.1 Establishment in the EU 1.2.3 Principles Relating to Processing of Personal Data <ul style="list-style-type: none"> 1.2.3.1 Lawfulness, Fairness, and Transparency 1.2.3.2 Purpose Limitation

- 1.2.3.3 Data Minimisation
 - 1.2.3.4 Accuracy
 - 1.2.3.5 Storage Limitation
 - 1.2.3.6 Integrity & Confidentiality
 - 1.2.3.7 Accountability
 - 1.2.4 Lawfulness of processing
 - 1.2.4.1 Consent
 - 1.2.4.2 Contract
 - 1.2.4.3 Legal Obligation
 - 1.2.4.4 Vital Interest
 - 1.2.4.5 Public Interest
 - 1.2.4.6 Legitimate Interest
 - 1.2.5 Processing of Special Categories of Personal Data and Data Relating to Criminal Convictions and Offences
 - 1.3 Rights of the Data Subject
 - 1.3.1 The Right to Be Informed
 - 1.3.2 The Right of Access
 - 1.3.3 The Right to Rectification
 - 1.3.4 The Right to Erasure
 - 1.3.5 The Right to Restrict Processing
 - 1.3.6 The Right to Data Portability
 - 1.3.7 The Right to Object
 - 1.3.8 Rights in Relation to Automated Decision Making and Profiling
 - 1.4 Controller and Processor
 - 1.4.1 Responsibilities of the Controller
 - 1.4.1.1 Joint Controller
 - 1.4.2 Responsibilities of the Processor
 - 1.4.3 Security of Personal Data
 - 1.4.4 Data Protection Impact Assessment
 - 1.4.5 Data Protection Officer
 - 1.4.6 Code of Conduct and Certification
 - 1.5 Transfers of Personal data to 3rd Countries or International Organisations
 - 1.5.1 General Principles for Transfers and Appropriate Safeguards
 - 1.5.2 Adequacy Decision
 - 1.5.3 Standard Contractual Clauses (SCCs)
 - 1.5.4 Binding Corporate Rules (BCRs)
 - 1.5.5 Derogations for Specific Situations
 - 1.5.6 International Cooperation
 - 1.5.6.1 Schrems 1 & 2 cases

		<p style="text-align: right;">1.5.6.2 Trans-Atlantic Data Privacy Framework</p> <p>1.6 Supervisory Authorities</p> <ul style="list-style-type: none"> 1.6.1 Independent Status 1.6.2 Rules on Establishment of the Supervisory Authority 1.6.3 Competence, Tasks, and Powers 1.6.4 Lead Supervisory Authority 1.6.5 Joint Operations of Supervisory Authorities 1.6.6 European Data Protection Board 1.6.7 European Data Protection Supervisor (EDPS) <p>1.7 Remedies, Liability, and Penalties</p> <ul style="list-style-type: none"> 1.7.1 Lodging a Complaint <ul style="list-style-type: none"> 1.7.1.1 Right to an Effective Judicial Remedy 1.7.1.2 Representation of Data Subject 1.7.2 Data Subject Compensation 1.7.3 Administrative Fines 1.7.4 Penalties
<p>Domain B <i>Compliance Mechanisms</i></p>	<p>Data protection policies, processes, and procedures</p>	<p>2.1 Data Protection Enabling Policies, Processes, and Procedures</p> <ul style="list-style-type: none"> 2.1.1 Privacy Documentation 2.1.2 Onboarding and Offboarding Procedures 2.1.3 Global IT Policy 2.1.4 Password Policy 2.1.5 Access Control Policy <p>2.2 Data Management</p> <ul style="list-style-type: none"> 2.2.1 Data Inventory, Data Classification, and Records of Processing Activities (RoPA) 2.2.2 Data Governance through Data Life Cycle 2.2.3 Data Breach Management 2.2.4 Data Flows Including International Data Transfers <ul style="list-style-type: none"> 2.2.4.1 Data Transfer Impact Assessment (TIA) <p>2.3 Compliance Monitoring and Audit</p> <ul style="list-style-type: none"> 2.3.1 Compliance Team Action Plan 2.3.2 Verification of Implementation and Operationalisation of the Relevant Policies and Procedures 2.3.3 Proofs of Accountability 2.3.4 Audit Plan
<p>Domain C <i>Information Security</i></p>	<p>Information security for data protection assessment and guidance</p>	<p>3.1 Pillars of Information Security</p> <p>3.2 Open Systems Interconnection (OSI) Model</p> <ul style="list-style-type: none"> 3.2.1 Data Protection at the Physical Layer (Layer 1) <ul style="list-style-type: none"> 3.2.1.1 Physical Security

- 3.2.1.2 Supervisory Control and Data Acquisition (SCADA) systems
- 3.2.1.3 Cable Integrity and Maintenance
- 3.2.1.4 Physical Layer Access Controls
- 3.2.1.5 Physical Layer Redundancy
- 3.2.1.6 Shielding against Electromagnetic Interference (EMI) and Radio-Frequency Interference (RFI)
- 3.2.1.7 Environmental Controls
- 3.2.1.8 Sniffing – Monitoring
- 3.2.1.9 Cryptography
- 3.2.1.10 Data Erasure and Destruction
- 3.2.2 Data Protection at the Data Link Layer (Layer 2)
 - 3.2.2.1 Segmentation at the Data Link Layer
- 3.2.3 Data Protection at the Network Layer (Layer 3)
 - 3.2.3.1 Network Layer Attacks
 - 3.2.3.2 Segmentation at Network Layer
 - 3.2.3.3 Example of Switched Networks: Local Area Network (LAN)
 - 3.2.3.4 Miniaturisation and Network Connectivity
 - 3.2.3.5 Software-Defined Networking (SDN) Network Segmentation
 - 3.2.3.6 Encryption Protocols at Network Layer
- 3.2.4 Data Protection at the Transport Layer (Layer 4)
 - 3.2.4.1 Transport Layer Attacks
 - 3.2.4.2 Server Message Block (SMB)
 - 3.2.4.3 Encryption Protocol at Transport Layer: Secure Sockets Layer (SSL) & Transport Layer Security (TLS)
- 3.2.5 Data Protection at the Session Layer (Layer 5)
 - 3.2.5.1 Session Expiration Time
 - 3.2.5.2 HTTP Headers
 - 3.2.5.3 Session Tokens
 - 3.2.5.4 Session Layer Attacks
- 3.2.6 Data Protection at the Presentation Layer (Layer 6)
 - 3.2.6.1 Presentation Layer Attacks
- 3.2.7 Data Protection at the Application Layer (Layer 7)
 - 3.2.7.1 Application Layer Protocols
 - 3.2.7.2 Application Layer Data Protection Measures
 - 3.2.7.3 Application Layer Attacks
 - 3.2.7.4 Vital Intersection of DNS and Privacy

3.3 Cloud Computing

		<ul style="list-style-type: none"> 3.3.1 Cloud Service Models (SaaS, PaaS, IaaS) 3.3.2 Cloud Deployment Models (public cloud, private cloud, etc.) 3.4 Identity and Access Management (IAM) <ul style="list-style-type: none"> 3.4.1 Digital Identity 3.4.2 Identity Management (IDM) 3.4.3 Authentication 3.4.4 Authorisation 3.4.5 Privileged Access Management (PAM) 3.4.6 Access Control 3.4.7 Cloud Access Security Brokers (CASBs) 3.4.8 Zero Trust 3.4.9 Microsoft Active Directory (AD) & Entra 3.5 Privacy Enhancing Technologies (PETs) <ul style="list-style-type: none"> 3.5.1 Anonymisation 3.5.2 K-Anonymity 3.5.3 Pseudonymisation 3.5.4 Encryption 3.5.5 Differential Privacy (DP) 3.5.6 Homomorphic Encryption 3.5.7 Private Set Intersection (PSI) 3.5.8 Onion Routing 3.5.9 Zero-Knowledge Proofs 3.5.10 Secure Multi-Party Computation 3.5.11 Federated Learning 3.5.12 Secure Sockets Layer (SSL) & Transport Layer Security (TLS) 3.5.13 End-to-End Encryption (E2EE) 3.5.14 Data Masking / Data Obfuscation 3.5.15 Cryptographic Algorithms 3.5.16 Privacy-Enhancing Technologies via Applied Cryptography Engineering (PETAce) 3.6 Privacy Engineering 3.7 Attack Surface Reduction (ASR) and Mitigation 3.8 Information Security Standards and Frameworks
<p>Domain D <i>Action Plan – How</i></p>	<p>Risk, impact assessment, and action plan</p>	<ul style="list-style-type: none"> 4.1 Risk Management <ul style="list-style-type: none"> 4.1.1 Privacy Threats and Vulnerabilities 4.1.2 Risk Assessment 4.1.3 Privacy Risk Models and Frameworks 4.1.4 Risk Management Strategies and Their Implementation <ul style="list-style-type: none"> 4.1.4.1 Avoidance 4.1.4.2 Mitigation 4.1.4.3 Sharing/Transfer

		<ul style="list-style-type: none"> 4.1.4.4 Acceptance 4.1.5 3rd Party Risk Management 4.2 Privacy Metrics <ul style="list-style-type: none"> 4.2.1 Management and Performance Indicators 4.2.2 Define Maturity Model 4.2.3 Data Protection Metrics 4.3 Data Protection Impact Assessment (DPIA) 4.4 Business Continuity <ul style="list-style-type: none"> 4.4.1 Disaster and Continuity Plan 4.5 Data Protection by Design and by Default <ul style="list-style-type: none"> 4.5.1 Privacy by Design 4.6 Management Platforms/Software
<p>Domain E <i>Privacy Culture – Human Perspective</i></p>	Data subject approach issues, (inter)personal skills of future DPOs, and ethical issues	<ul style="list-style-type: none"> 5.1 RACI 5.2 Privacy Trainings and Awareness 5.3 Code of Conduct 5.4 Certification 5.5 Privacy Challenges of Technology <ul style="list-style-type: none"> 5.5.1 Tracking and Surveillance 5.5.2 Smart Cities 5.5.3 IoTs 5.5.4 Automated Decision Making 5.5.5 AI and Ethical Issues

7. Exam Blueprint

	Domain A: European Data Protection Legislation	Domain B: Compliance Mechanisms	Domain C: Information Security	Domain D: Action Plan	Domain E: Privacy Culture
Weight %	60%	15%	10%	10%	5%
# questions	24	6	4	4	2

8. Exam Preparation

Preparing for the EADPP Certification exam is a crucial step in a candidate's journey as a certified data protection professional. Professional starters will acquire essential knowledge and skills during their preparation, while more seasoned professionals can assess whether their expertise is sufficient to address challenges related to implementing a privacy culture.

Since the exam evaluates knowledge and understanding of privacy concepts, principles, and practices outlined in the Privacy Enablers' Body of Knowledge and Skills (BOKS) (see Section 8), early preparation is highly recommended. The number of study and training hours required depends on the candidate's prior knowledge and work experience with the five principal domains summarized in the BOKS.

There are multiple ways to prepare effectively:

- Review the Privacy Enablers' BOKS to understand the scope and depth of the material covered in the exam. Candidates should study each domain thoroughly and familiarize themselves with the relevant concepts, principles, and practices.
- Supplement with additional resources such as books, articles, and web content to deepen understanding. It is essential to ensure that these materials are up-to-date and relevant to the Certification.
- Participate in training provided by Privacy Enablers' Acknowledged Training Partners. These structured trainings can help candidates identify areas where additional study is needed and ensure comprehensive coverage of all domains in the BOKS.

By following a structured approach—reviewing the BOKS, leveraging additional resources, and considering professional training—candidates can increase their chances of successfully passing the exam. Privacy Enablers' Acknowledged Training Partners offer [tailored trainings](#) to assist candidates in their preparation, ensuring an effective and thorough learning experience.