PRIVACY ENABLERS
DATA PROTECTION X CERTIFICATION

EADPP
european association of data protection professionals

EADPP Certification for Data Protection Professionals

Syllabus

Version 1.0

1. About EADPP

EADPP (European Association of Data Protection Professionals) is the first independent European non-profit organization 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 organizations, think tanks, and academia 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 Privacy Enablers' Certification scheme, and to create a professional network for cooperation. The EADPP community is growing day by day, worldwide[1].

2. Why a European 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 General Data Protection Regulation (GDPR) being a landmark achievement. It is an inclusive Certification program, developed and managed by European data professionals, welcoming participation from Data Protection Professionals worldwide. Non-EU professionals and organizations can greatly benefit from the EADPP Certification as it provides them with valuable insights into the EU data protection and privacy culture, enabling them to navigate compliance requirements when dealing with EU personal data processing.

[1] Follow EADPP on LinkedIn.

3. Aim of the EADPP Certification

There is no privacy without cybersecurity. A Data Protection Professional with expertise in both areas can help organizations develop more effective risk management strategies. By understanding both the privacy and cybersecurity risks faced by organizations, a Data Protection Professional can help develop policies and procedures that are more effective in protecting data and mitigating risk.

A Data Protection 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 on 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.

A Data Protection Professional who successfully completes the EADPP Certification, demonstrates their ability to ensure high-quality implementation of data protection measures beyond the legal aspects.

4. Certificate & Training Hours

Professional starters will acquire much needed necessary knowledge and skills during the preparation for the Certification exam. More seasoned professionals will verify if their knowledge and skills are sufficient to address challenges related to the implementation of a privacy culture. For both, the Certification is considered a

major step in the journey of self-development of the candidate as a Data Protection Professional.

The recommended number of learning and training hours depends on the candidate's prior knowledge of and/or work experience with the five principal domains summarized in the Privacy Enablers' Body of Knowledge and Skills (BOKS; see section 8).

Privacy Enablers' acknowledged training partners can support the candidate with tailored trainings.

5. Exam Information

Type of exam	Multiple-choice questions
Number of questions	40 questions
Exam duration	120 minutes
Passing grade or mark	28/40
Method of delivery	Computer-based: - Test center; or - Remote proctored

6. Additional Benefits

The successful candidate receives a free one (1)-year membership of EADPP, including these member benefits:

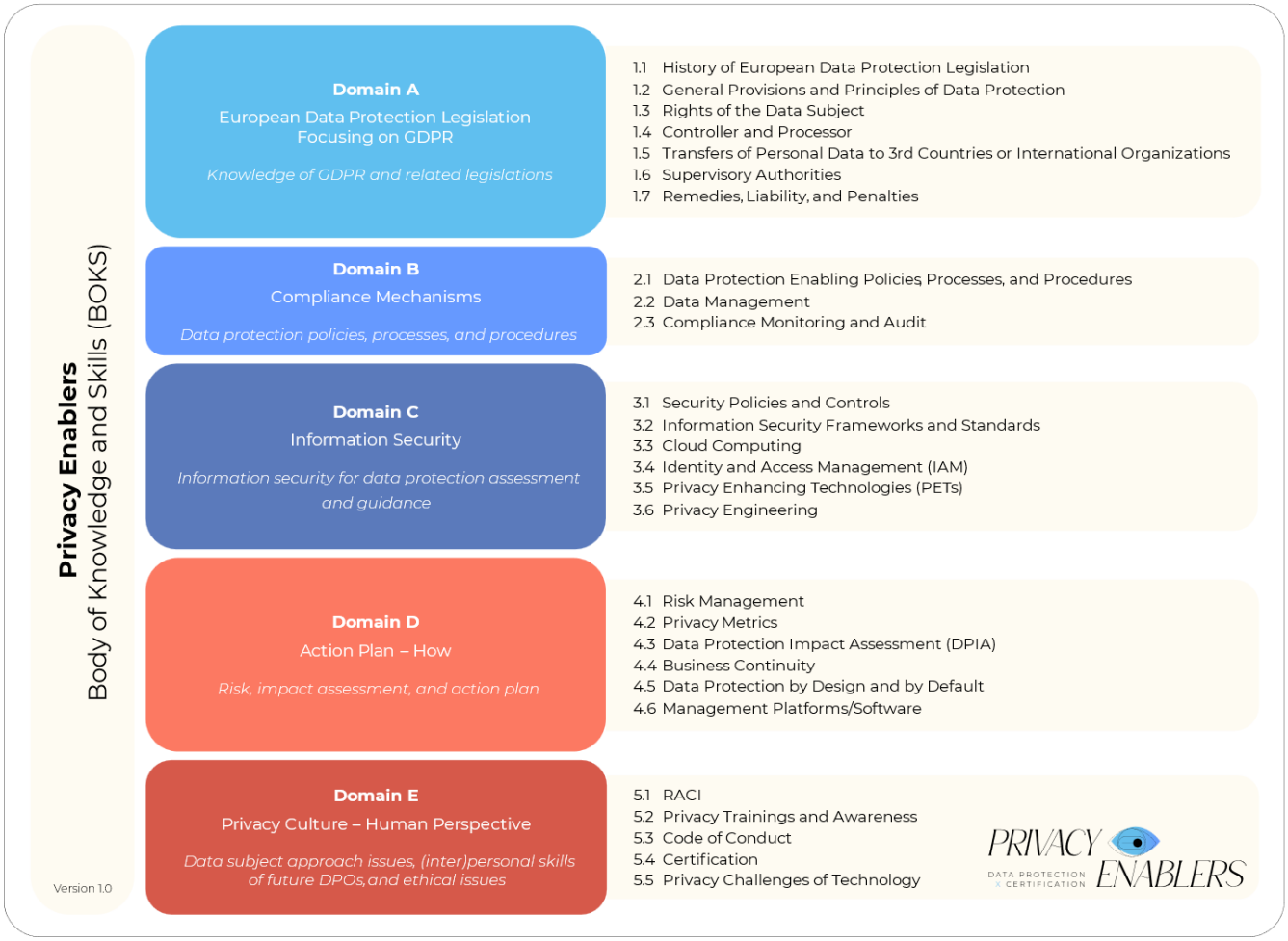
- Globally connected peer network: Be inspired by like-minded professionals of the EADPP Community of Data Protection Professionals and expand your network worldwide;

- Career boost: Endorse your professional skills through the Certification for Data Protection Professionals, boosting your profile to employers;
- As an EADPP member, you benefit from discounted rates on Certification and trainings.

7. 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	- Understand the evolution of European data protection legislation - Know GDPR concepts	- Understand the require-ments for GDPR compliance - Basic concepts of data governance	Understand basic principles of information security	- 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 program

8. Certificate Content – Privacy Enablers Body of Knowledge and Skills (BOKS)



Domain	*Scope*	*Sub-domains*
Domain A *European Data Protection Legislation Focusing on GDPR*	Knowledge of GDPR and related legislations	1.1 History of European Data Protection Legislation 1.1.1 OECD Guidelines 1.1.2 Convention 108 1.2 General Provisions and Principles of Data Protection 1.2.1 Material Scope 1.2.2 Territorial Scope 1.2.2.1 Establishment in the EU 1.2.3 Principles Relating to Processing of Personal Data 1.2.3.1 Lawfulness, Fairness, and Transparency 1.2.3.2 Purpose Limitation 1.2.3.3 Data Minimization

		1.5.6.2 Trans-Atlantic Data Privacy Framework 1.6 Supervisory Authorities 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) 1.7 Remedies, Liability, and Penalties 1.7.1 Lodging a Complaint 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
Domain B *Compliance Mechanisms*	Data protection policies, processes, and procedures	2.1 Data Protection Enabling Policies, Processes, and Procedures 2.1.1 Creating Privacy Notes and Forms 2.1.2 Onboarding and Offboarding Procedures 2.1.3 Global IT Policy 2.1.4 Password Policy 2.1.5 Access Control Policy 2.2 Data Management 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 2.2.4.1 TIA - Data Transfer Impact Assessment 2.3 Compliance Monitoring and Audit 2.3.1 Compliance Team Action Plan 2.3.2 Verification of Implementation and Operationalization of the Relevant Policies and Procedures 2.3.3 Proofs of Accountability 2.3.4 Audit Plan
Domain C *Information Security*	Information security for data protection assessment and guidance	3.1 Security Policies and Controls 3.1.1 Encryption 3.1.2 PKI (Public Key Infrastructure) 3.1.3 Hashing 3.2 Information Security Frameworks and Standards

		3.2.1 NIST Framework 3.2.2 ISO 27000 Range, in particular ISO27001: 2022 (Standard for Information Security Management Systems, ISMS) 3.2.3 ISO 27701 (Privacy Information Management System, PIMS) 3.2.4 COBIT (ISACA) 3.3 Cloud Computing 3.3.1 Cloud Service Models 1.3.1.1 Saas 1.3.1.2 Paas 1.3.1.3 Iaas 3.3.2 Cloud Deployment Models 3.3.2.1 Public Cloud 3.3.2.2 Private Cloud 3.3.2.3 Hybrid Cloud 3.3.3 Contractual Aspects 3.4 Identity and Access Management (IAM) 3.4.1 Identity Management 3.4.2 Authentication 3.4.3 Authorization 3.4.4 Privileged Access Management (PAM) 3.4.5 Access Control 3.4.6 Zero Trust 3.5 Privacy Enhancing Technologies (PETs) 3.5.1 Anonymization 3.5.2 Pseudonymization 3.5.3 Encryption (SSL, TLS, ...) 3.5.4 Cryptographic Algorithms 3.5.4.1 Homomorphic Encryption 3.5.4.2 Secure multi-party computation (SMPC) 3.5.4.3 Differential Privacy 3.5.4.4 Zero-Knowledge Proofs 3.5.5 Synthetic Data 3.5.6 Federated Learning 3.5.7 Access Control 3.5.8 VPNs/Geo-Blocking 3.6 Privacy Engineering
Domain D *Action Plan – How*	Risk, impact assessment,	4.1 Risk Management 4.1.1 Privacy Threats and Vulnerabilities 4.1.2 Risk Assessment 4.1.3 Privacy Risk Models and Frameworks

	and action plan	4.1.4 Risk Management Strategies and Their Implementation 4.1.4.1 Avoidance 4.1.4.2 Mitigation 4.1.4.3 Sharing/Transfer 4.1.4.4 Acceptance 4.1.5 3rd Party Risk Management 4.2 Privacy Metrics 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 4.4.1 Disaster and Continuity Plan 4.5 Data Protection by Design and by Default 4.5.1 Privacy by Design 4.6 Management Platforms/Software
Domain E *Privacy Culture – Human Perspective*	Data subject approach issues, (inter)personal skills of future DPOs, and ethical issues	5.1 RACI 5.1.1 Defining Roles and Responsibilities 5.2 Privacy Trainings and Awareness 5.3 Code of Conduct 5.4 Certification 5.5 Privacy Challenges of Technology 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

9. How to Prepare for the Exam

If you are planning to take the EADPP Certification exam, it is important to start your preparation early. The exam assesses your knowledge and understanding of privacy concepts, principles, and practices as outlined in the Privacy Enablers' Body of Knowledge and Skills (BOKS) developed for the Certification program. Therefore, you need to ensure that you have a thorough understanding of the topics of the Privacy Enablers' BOKS before taking the exam.

There are multiple ways to prepare for the EADPP Certification exam:

- The first and most obvious is to review the content of the provided Privacy Enablers' BOKS. This will help you to understand the scope and depth of the material that will be tested on the exam. You should study each of the domains of the Privacy Enablers' BOKS and familiarize yourself with the concepts, principles, and practices described in each domain;
- In addition to the resources provided by EADPP, you may want to review other sources such as books, articles, and web content to supplement your understanding of the material. You should ensure that the resources you use are up-to-date and relevant to the Certification program; and
- Participating in a training with Privacy Enablers' acknowledged Training Partners is an excellent way to prepare for the exam. Their training programs provide a structured approach to learning the material and can help you to identify areas where you may need additional study. You should ensure that the training program you choose is designed specifically for the EADPP Certification exam and covers all of the domains in the Privacy Enablers' BOKS.

In summary, to prepare for the EADPP Certification exam, you should review the Privacy Enablers' BOKS, review other relevant resources, and consider participating in a training with Privacy Enablers' acknowledged Training Partners. By taking a structured approach to your preparation, you can increase your chances of passing the exam and earning the Certification.

10. 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%
Average # questions	24	6	4	4	2