Preparation Guide

Edition 201809

Content

1. Overview

EXIN Privacy & Data Protection Practitioner (PDPP.EN)

Scope

The EXIN Privacy & Data Protection Practitioner is a certification that validates a professional's knowledge and understanding of the European privacy (data protection) legislation and its international relevance as well as his or her ability to apply this knowledge and understanding in everyday professional practice.

Summary

With the ever increasing explosion of information flooding the internet, every company needs to plan how to manage and protect privacy of persons and their data. Not without a reason, many new laws - in the EU as well as in the USA and many other regions - are being formed in order to regulate both.
The European Commission has just published the EU General Data Protection Regulation (GDPR), meaning that all organizations concerned need to comply with specific rules. This Practitioner certification builds on the subjects covered by the Foundation exam by focusing on the development and implementation of policies and procedures in order to comply with existing and new legislation, application of privacy and data protection guidelines and best practices, and by establishing a Data and Privacy Protection Management System.

Context

The certificate EXIN Privacy & Data Protection Practitioner (PDPP) is part of the qualification program EXIN Privacy & Data Protection.

Target group

This Practitioner level certification will be particularly useful to Data Protection Officers (DPOs) / Privacy Officers, Legal / Compliance Officers, Security Officers, Business Continuity Managers, Data Controllers, Data Protection Auditors (internal and external), Privacy Analyst and HR managers.
As this is an advanced-level certification, it is highly recommended to previously have successfully passed EXIN Privacy & Data Protection Foundation.

Requirements for certification

- Accredited Privacy & Data Protection Practitioner training, including successful completion of the Practical Assignments;
- Successful completion of the EXIN Privacy & Data Protection Practitioner exam.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40
Pass mark:	65%
Open book/notes:	No, with the exception of literature C. Literature C may be consulted throughout the exam. It is provided as appendix to the digital exam. Please bring your own copy if the exam takes place on paper.
Electronic equipment/aides permitted:	No
Time allotted for examination:	120 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Bloom level

The EXIN Privacy & Data Protection Practitioner certification tests candidates at Bloom Level 2, 3 and Level 4 according to Bloom's Revised Taxonomy:

- Bloom Level 2: Understanding – a step beyond remembering (Level 1). Understanding shows that candidates can comprehend what is presented and can evaluate how the learning material may be applied in their own environment.
  This type of questions aims to demonstrate that the candidate is able to organize, compare, interpret and choose the correct description of facts and ideas.
- Bloom Level 3: Applying – shows that candidates have the ability to make use of information in a context different from the one in which it was learned.
  This type of questions aims to demonstrate that the candidate is able to solve problems in new situations by applying acquired knowledge, facts, techniques and rules in a different, or new way. The question usually contains a short scenario
- Bloom level 4: Analyzing – shows that candidates have the ability to break learned information into its parts to understand it. This Bloom level is mainly tested in the Practical Assignments. The Practical Assignments aim to demonstrate that the candidate is able to examine and break information into parts by identifying motives or causes, make inferences and find evidence to support generalizations..

Training

Contact hours

The recommended number of contact hours for this training course is 21. This includes (group) assignments, exam preparation and short breaks. This number of hours does not include homework, practical assignments, the exam session and lunch breaks. The recommended numbers of hours for the Practical Assignments is a maximum of 8. The Practical Assignments can be completed outside of the training. They may also be included in the training if the training duration is extended.
If the training provider wishes to dedicate time to national privacy and data protection legislation, this will require extra training hours in addition to the 21 recommended training hours.

Indication study effort

120 hours, depending on existing knowledge.

Training organization

You can find a list of our accredited training organizations at www.exin.com.

2. Exam requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam requirement	Exam specification	Weight
1. Data Protection Policies		**10%**
	1.1 Purpose of the Data Protection/Privacy Policies within an Organization	5%
	1.2 Data Protection by Design and by Default	5%
2. Managing and Organizing Data Protection		**35%**
	2.1 Phases of the Data Protection Management System (DPMS)	35%
	2.2 Action Plan for Data Protection Awareness [1]	0%
3. Roles of the Controller, Processor and Data Protection Officer (DPO)		**15%**
	3.1 Roles of the Controller and Processor	7.5%
	3.2 Role and Responsibilities of a DPO	7.5%
4. Data Protection Impact Assessment (DPIA)		**30%**
	4.1 Criteria for a DPIA	15%
	4.2 Steps of a DPIA	15%
5. Data Breaches, Notification and Incident Response		**10%**
	5.1 GDPR Requirements with Regard to Personal Data Breaches	5%
	5.2 Requirements for Notification	5%
	Total	100%

[1] Exam requirement 2.2 is not included in the exam, as there is no suitable reference material available yet. Exam questions about this specification will be added in a later version.

Exam specifications

1 Data Protection Policies

1.1 Purpose of the Data Protection/Privacy Policies within an Organization

The candidate can …

1.1.1 explain the policies and procedures needed within an organization to comply with data protection legislation

1.1.2 explain the content of the policies

1.2 Data Protection by Design and by Default

The candidate can ….

1.2.1 explain the concept of data protection by design and by default

1.2.2 describe the Seven principles for data protection by design and by default

1.2.3 illustrate how principles of privacy by design and by default can be implemented

2 Managing and Organizing Data Protection

2.1 Phases of the Data Protection Management System (DPMS)

The candidate can …

2.1.1 illustrate how to apply phase 1 of the DPMS: Data Protection and Privacy: Preparation

2.1.2 illustrate how to apply phase 2 of the DPMS: Data Protection and Privacy: Organization

2.1.3 illustrate how to apply phase 3 of the DPMS: Data Protection and Privacy: Development and Implementation

2.1.4 illustrate how to apply phase 4 of the DPMS: Data Protection and Privacy: Governance

2.1.5 illustrate how to apply phase 5 of the DPMS: Data Protection and Privacy: Evaluation and Improvement

2.2 Action Plan for Data Protection Awareness [2]

The candidate can ….

2.2.1 compose an action plan for data protection awareness in a specific situation

3 Roles of the Controller, Processor and Data Protection Officer (DPO)

3.1 Roles of the Controller and Processor

The candidate can …

3.1.1 enact the responsibilities of the controller

3.1.2 enact the responsibilities of the processor

3.1.3 explain the relationship between the controller and the processor in a specific situation

3.2 Role and Responsibilities of a DPO

The candidate can …

3.2.1 explain when a DPO is mandatory under the GDPR

3.2.2 enact the role of the DPO

3.2.3 explain the position of the DPO in relation to the supervisory authority[3]

[2] Exam requirement 2.2 is not included in the exam, as there is no suitable reference material available yet. Exam questions about this specification will be added in a later version.

[3] Before the GDPR was introduced the *data protection authority* was the national authority in EU countries, in charge of the enforcement of regulation on data protection. In the GDPR it is now called the *supervisory authority*.

4 Data Protection Impact Assessment (DPIA)

4.1 Criteria for a DPIA

The candidate can …

4.1.1 apply the criteria for conducting a DPIA

4.1.2 describe the objectives and outcomes of a DPIA

4.2 Steps of a DPIA

The candidate can …

4.2.1 describe the steps of a DPIA

4.2.2 perform a DPIA in a specific situation

5 Data Breaches, Notification and Incident Response

5.1 GDPR Requirements with Regard to Personal Data Breaches

The candidate can …

5.1.1 assess whether a data breach has taken place in terms of the GDPR

5.2 Requirements for Notification

The candidate can …

5.2.1 notify the supervisory authority of a personal data breach

5.2.2 notify the data subject of the personal data breach

5.2.3 describe the elements of the GDPR documentation obligation

3. List of Basic Concepts

This chapter contains the terms and abbreviations with which candidates should be familiar.

Please note that knowledge of these terms alone does not suffice for the exam; the candidate must understand the concepts and be able to provide examples

- adequate
- appropriate technical and organizational measures
- audit
  - initial data (protection) audit
  - internal and external data (protection) audit
- authenticity
- availability
- awareness
- benchmark
- binding
- binding corporate rules
- biometric data
- Bring Your Own Device (BYOD)
- certification
- certification bodies
- child's consent
- cloud computing
- codes of conduct
- collection of personal data (verb.)
- commission reports
- Complaint
- Compliance
- conditions for consent
- Consent
- Consistency
- consistency mechanism
- Constitution
- Contract
- Controller
- cross-border processing
- data accuracy
- data breach
- data classification system
- data concerning health
- data controller
- data lifecycle management (DLM)
- data mapping
- data portability
- data protection
- (data privacy) breach response plan / data privacy incident response plan
- data protection authority (DPA)
- data protection by default / privacy by default
- data protection by design / privacy by design
- data protection impact assessment (DPIA) / privacy impact assessment (PIA)
- Data Protection Management System (DPMS) / Data Protection and Privacy Management System (DPMS)
- data protection officer (DPO)
  - designation
  - position
  - tasks
- data protection policy
- data protection program
- data protection provisions
- data subject
- data subject access (facilities)
- data transfer
- declaration of consent
- delegated acts and implementing acts
  - committee procedure
- documentation obligation
- Derogation

Enforcement
- administrative fines
- administrative penalties
- criminal penalties
- dissuasive penalties
- effective penalties
- proportionate penalties

Enterprise

European Economic Area (EEA)

EU types of legal act
- decision
- directive
- opinion
- recommendation
- regulation

European Data Protection Board
- chair
- confidentiality
- independence
- procedure
- reports
- secretariat
- tasks

European Data Protection Supervisor (EDPS)

European Union legal acts on data protection

exchange of information

Exemption

explicit consent

filing system

General Data Protection Regulation (GDPR)

genetic data

governing body

group of undertakings

incident response

independent supervisory authorities
- activity reports
- competence
- establishment
- powers
- tasks

Information Security Management System (ISMS)

information society service

international organization

Internet of Things (IOT)

joint controllers

judicial remedy

lawfulness of processing

legal basis

legitimate ground (GDPR art. 17/1c, art. 18/1d, art. 21/1) and legitimate basis (GDPR art. 40)

legitimate interest

liability

main establishment

material scope

measures based on DPIA results

National Identification Number

non-repudiation

notification obligation

opinion of the board

personal data

personal data breach

personal data relating to criminal convictions and offences

principles relation to processing of personal data (Lit. C GDPR, art. 5)
- accountability
- accuracy
- confidentiality
- data minimization
- fairness
- integrity
- lawfulness
- purpose limitation
- storage limitation
- transparency

policy

policy rule(s)

prior consultation

privacy

privacy analysis

privacy officer/chief privacy officer

processing

processing (of personal data)

processing agreement

processing situations
- data protection rules of churches and religious associations
- employment
- for archiving purposes in the public interest
- for scientific or historical research purposes
- for statistical purposes
- freedom of expression and information
- National Identification Number
- obligations of secrecy
- public access to official documents

processing which does not require identification

processor

profiling

proportionality, the principle of

pseudonymization

quality cycle

recipient

relevant and reasoned objection

repealed

representative

restriction of processing

retention period

right to compensation

rights of the data subject
- automated individual decision-making
- data portability
- information and access
- modalities
- notification obligation
- rectification and erasure
- restriction of processing
- restrictions
- 'right to be forgotten'
- right to objection
- transparency

risk management

rules of procedure

security breach (security incident)

security of personal data

security of processing

sensitive data

service provider

seven principles for privacy by design

Social, Mobile, Analytics, Cloud, Things (SMACT)

special categories of personal data
- biometric data
- data concerning health
- genetic data
- political opinions
- racial or ethnic origin
- religious or philosophical beliefs
- sex life or sexual orientation
- trade union membership

subsidiarity, the principle of

supervisory authority

supervisory authority concerned

suspension of proceedings

territorial scope

third party

threat

Transfer of personal data to third countries and to international organizations
- adequacy decision
- appropriate safeguards
- binding corporate rules
- derogations
- disclosures
- international protection of personal data

vullnerability

unified communications and collaboration (UCC)

4. Literature

Exam literature

The knowledge required for the EXIN Privacy & Data Protection Practitioner exam is covered in the following literature:

A. IT Governance Privacy Team
EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide
IT Governance Publishing, Cambridgeshire (2016)
ISBN 978-1-84928-8354 (paperback)
ISBN 978-1-84928-8378 (e-book)

B. Kyriazoglou, J.
Data Protection and Privacy Management System. Data Protection and Privacy Guide - Vol. 1
bookboon.com 1st edition (2016)
ISBN 978-87-403-1540-0

C. European Commission
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016, available at http://eur-lex.europa.eu
PDF:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
HTML:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN

D. Article 29 Data Protection Working Party
Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01, 5 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

E. Article 29 Data Protection Working Party
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248, 4 April 2017 available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Comment

The exam requirements are based on the exam literature. Literature C is no primary exam literature because the other exam literature provides sufficient content about the GDPR. Candidates should be familiar with literature C to the extent of the references made in the other literature. Literature C may be consulted throughout the exam. It is provided as appendix to the digital exam. Please bring your own copy if the exam takes place on paper.

Additional literature

F. Example of Privacy by Design Framework
https://www.privacycompany.eu/files/DPbD_Framework.pdf

Comment

Additional literature is for reference and depth of knowledge only.

Literature matrix

Exam requirement	Exam specification	Literature
1. Data Protection Policies		
	1.1 Purpose of the Data Protection/Privacy Policies within an Organization	A: Chapter 16 paragraph Using policies to demonstrate compliance
	1.2 Data Protection by Design and by Default	A: Chapter 5 paragraph Privacy by design and by default
2. Managing and Organizing Data Protection		
	2.1 Phases of the Data Protection Management System (DPMS)	A: Chapter 12 paragraph Records of processing A: Chapter 14 introduction + paragraph Notification B: Chapter 2, paragraph 2 DP&P System Phases
	2.2 Action Plan for Data Protection Awareness	*No literature yet*
3. Roles of the Controller, Processor and Data Protection Officer (DPO)		
	3.1 Roles of the Controller and Processor	A: Chapter 12
	3.2 Role and Responsibilities of a DPO	A: Chapter 2 B: Chapter 2 paragraph 2 Phase 4 D: Chapter 2 paragraph 1 Mandatory designation D: Chapter 4 Tasks of the DPO D: Chapter 5 paragraph 1 Which organizations must appoint a DPO?
4. Data Protection Impact Assessment (DPIA)		
	4.1 Criteria for a DPIA	A: Chapter 5 introduction, paragraph Privacy Impact Assessments and paragraph When to conduct a DPIA A: Chapter 6 paragraph DPIA's as part of risk management A: Chapter 8 paragraph Objectives and outcomes E: Chapter 3 DPIA: the Regulation explained

	4.2 Steps of a DPIA	A: Chapter 5 paragraph Privacy Impact Assessments A: Chapter 7 A: Chapter 8 paragraph Five key stages in a DPIA and paragraph Consultation E: Chapter 3 DPIA: the Regulation explained
5. Data Breaches, Notification and Incident Response		
	5.1 GDPR Requirements with Regard to Personal Data Breaches	A: Chapter 3 paragraph Personal data breaches, Anatomy of a data breach, Sites of attack
	5.2 Requirements for Notification	A: Chapter 14 paragraph Notification, paragraph Events vs incidents, paragraph Types of incidents

Comment

Literature C, the GDPR, is not referenced in detail.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER