Preparation Guide

Edition 202403

Content

1. Overview

EXIN Privacy & Data Protection Professional (PDPP.EN)

Scope

EXIN Privacy & Data Protection Professional is a certification that validates a professional's knowledge about:

- data protection policies
- privacy information management systems (PIMSs)
- roles of the controller, processor and data protection officer (DPO)
- data protection impact assessment (DPIA)
- data breaches, notification, and incident response

Summary

EXIN Privacy & Data Protection Professional covers the European privacy and data protection legislation and its international relevance, as well as the professional's ability to apply this knowledge and understanding to everyday professional practice.

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 within the EU, as well as in the USA and many other regions, are formed to regulate both privacy and data protection.

The European Commission has published the EU General Data Protection Regulation (GDPR), meaning that from the 25th of May 2018 on, all organizations concerned must comply with specific rules. This advanced-level certification builds on the subjects covered by the EXIN Privacy & Data Protection Foundation exam by focusing on the development and implementation of policies and procedures to comply with existing and new legislation, application of privacy and data protection guidelines and best practices, and by establishing a data protection management system (DPMS).

The standard in the ISO/IEC 27000 series: ISO/IEC 27701:2019 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines is useful for organizations that want to show compliance with the GDPR. The content of this ISO standard helps fulfill the GDPR obligations of organizations regarding the processing of personal data.

Neither the GDPR nor the ISO standard are exam literature. However, the literature matrix in Chapter 4 is designed to show the link between the exam requirements, the exam literature, the GDPR and the ISO/IEC 27701:2019 standard to give the certification a broader context.

Context

The EXIN Privacy & Data Protection Professional certification is part of the EXIN Privacy & Data Protection qualification program.

Target group

This advanced-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 analysts
- HR-managers

Requirements for certification

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

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40
Pass mark:	65% (26/40 questions)
Open book:	The GDPR text may be consulted throughout the exam. It is provided as an appendix to the digital exam. Candidates are required to bring their own copy for paper-based exams.
Notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	120 minutes

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

Bloom level

The EXIN Privacy & Data Protection Professional certification tests candidates at Bloom levels 2, 3 and 4 according to Bloom's revised taxonomy:

- Bloom level 2: Understanding - a step beyond remembering. Understanding shows that candidates 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: Application - 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. These questions usually contain a short scenario.
- Bloom level 4: Analysis - shows that candidates have the ability to break learned information down 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 practical assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication study effort

112 hours (4 ECTS), 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 requirements	Exam specifications	Weight
1. Data protection policies		**10%**
	1.1 Purpose of data protection and privacy policies within an organization	5%
	1.2 Data protection by design and by default	5%
2. Privacy information management system (PIMS)		**32.5%**
	2.1 Privacy information management system (PIMS) basics	12.5%
	2.2 Benefits of a privacy information management system (PIMS)	10%
	2.3 Privacy information management system (PIMS) relationships	10%
3. Roles of the controller, processor, and data protection officer (DPO)		**17.5%**
	3.1 Roles of the controller and processor	10%
	3.2 Role and responsibilities of a data protection officer (DPO)	7.5%
4. Data protection impact assessment (DPIA)		**27.5%**
	4.1 Criteria for a data protection impact assessment (DPIA)	15%
	4.2 Steps of a data protection impact assessment (DPIA)	12.5%
5. Data breaches, notification, and incident response		**12.5%**
	5.1 GDPR requirements with regard to personal data breaches	2.5%
	5.2 Requirements for notification	10%
	Total	**100%**

Exam specifications

1 Data protection policies

1.1 Purpose of data protection and 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 Privacy information management system (PIMS)

2.1 Privacy information management system (PIMS) basics
The candidate can…
- 2.1.1 explain the different terms used in the ISO/IEC 27701 standard (internal and external issues, interested parties).
- 2.1.2 list which media must be considered when implementing a PIMS.
- 2.1.3 define what a statement of applicability (SoA) is.
- 2.1.4 explain the purpose of documentation in a PIMS.
- 2.1.5 explain the purpose of management reviews in a PIMS.

2.2 Benefits of a privacy information management system (PIMS)
The candidate can…
- 2.2.1 explain the objective of audits in a PIMS.
- 2.2.2 explain how to determine the specific requirements of a PIMS in light of the appropriate local rules and contractual requirements.
- 2.2.3 explain how a PIMS and audits help to show compliance with standards and regulations.
- 2.2.4 explain how a PIMS can help with supplier selection.

2.3 Privacy information management system (PIMS) relationships
The candidate can…
- 2.3.1 explain the difference between a privacy information management system (PIMS) and an information security management system (ISMS).
- 2.3.2 explain the relationship between the data protection principle of appropriate information security arrangements and the ISO/IEC 27701 standard.
- 2.3.3 explain the usefulness of the ISO/IEC 27002 standard for the implementation of a PIMS.
- 2.3.4 explain how to apply PIMS controls.

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 data protection officer (DPO)
The candidate can…
- 3.2.1 explain when appointment of 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.

4 Data protection impact assessment (DPIA)

4.1 Criteria for a data protection impact assessment (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 data protection impact assessment (DPIA)

The candidate can…

- 4.2.1 describe the steps of a DPIA.
- 4.2.2 perform a DPIA in specific situations.

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.

appropriate technical and organizational measures
audit
authenticity
availability
awareness
bring your own device (BYOD)
certification (bodies)
cloud computing
code of conduct
collecting personal data
commission reports
complaint
compliance
consent
- child's consent
- conditions for consent
- explicit consent

consistency mechanism
controller
cross-border processing
data accuracy
data breach
data classification system
data lifecycle management (DLM)
data mapping
data portability
data protection
data protection authority (DPA)
data protection by default / privacy by default
data protection by design / privacy by design
data protection impact assessment (DPIA)
data protection officer (DPO)
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
enforcement
EU types of legal act
European Data Protection Board
European Data Protection Supervisor (EDPS)
European Economic Area (EEA)
European Union legal acts on data protection
GDPR (General Data Protection Regulation)
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
legitimate basis (GDPR recital 40)
legitimate ground (GDPR Article 17(1c), Article 18(1d), Article 21(1))
legitimate interest
liability
main establishment
material scope
non-repudiation
notification obligation
opinion of the board
personal data
personal data breach
personal data relating to criminal convictions and offences
policy (rules)
principles relation to processing of personal data (GDPR, Article 5)
- accountability
- accuracy
- confidentiality
- data minimization
- fairness
- integrity
- lawfulness
- purpose limitation
- storage limitation
- transparency

prior consultation
privacy
privacy analysis
privacy information management system (PIMS)
privacy officer
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

processor
profiling
proportionality, the principle of
pseudonymization
quality cycle
recipient
relevant and reasoned objection
repealed
representative
restriction of processing
retention period
rights of the data subject
- 'right to be forgotten'
- automated individual decision-making
- data portability
- information and access
- modalities
- notification obligation
- rectification and erasure
- restriction of processing
- right to compensation
- right to objection
- transparency

risk management
rules of procedure
security breach
security incident
service provider
seven principles for privacy by design
Social [media], Mobile [technology], [advanced] Analytics, Cloud and [Internet of] 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 (BCR)
- derogations
- disclosures
- international protection of personal data

unified communications and collaboration (UCC)
vulnerability

4. Literature

Exam literature

The knowledge required for the 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 (4th edition, 2020)
ISBN 9781787782495 (pdf)
ISBN 9781787782501 (e-book)
ISBN 9781787782518 (Kindle)
ISBN 9781787782488 (hardcopy)
ISBN 9781787782495 (audiobook)

B. Alan Shipman & Steve Watkins
ISO/IEC 27701:2019: An introduction to privacy information management
IT Governance Publishing (2020)
ISBN: 9781787781993 (hardcopy)
ISBN: 9781787782013 (e-book)

Additional literature

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

D. Article 29 Data Protection Working Party
Guidelines on Data Protection Officers ('DPOs'), wp 243rev.01, 5 April 2017

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

F. A. Cavoukian
Privacy by Design – The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

G. ISO/IEC 27701:2019 (EN)
Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines
Switzerland, ISO/IEC (2019)
https://www.iso.org/home.html

Comment

Additional literature is for reference and depth of knowledge only.

The GDPR text (source C) is no primary exam literature because the exam literature provides sufficient knowledge about the GDPR. Candidates should be familiar with the references to the GDPR made in the other literature.

Literature Matrix

Exam requirements	Exam specifications	Literature reference	GDPR reference	ISO/IEC 27701 reference
1. Data protection policies				
	1.1 Purpose of data protection and privacy policies within an organization	A, Chapter 1, Chapter 16	*no reference*	*no reference*
	1.2 Data protection by design and by default	A, Chapter 5	Article 25	Section B.8.4, Subclause 6.11.2.1, Subclause 6.11.2.5, Subclause 7.4.2
2. Privacy information management system (PIMS)				
	2.1 Privacy information management system (PIMS) basics	B, Chapter 1, Chapter 2, Chapter 3, Chapter 4	*no reference*	*Full document*
	2.2 Benefits of a privacy information management system (PIMS)	B, Chapter 2, Chapter 3, Chapter 4, Chapter 5	*no reference*	*Full document*
	2.3 Privacy information management system (PIMS) relationships	B, Chapter 3, Chapter 4, Chapter 5, Chapter 6	*no reference*	*Full document*
3. Roles of the controller, processor, and data protection officer (DPO)				
	3.1 Roles of the controller and processor	A, Chapter 12	Article 24, Article 26, Article 27, Article 28, Article 29	Subclause 5.2.1, Subclause 6.3.1.1, Subclause 6.12.1.2, Subclause 6.15.1.1, Subclause 7.2.6, Subclause 7.2.7, Subclause 8.2.1, Subclause 8.2.4, Subclause 8.2.5, Subclause 8.5.4, Subclause 8.5.6, Subclause 8.5.7, Subclause 8.5.8
	3.2 Role and responsibilities of a data protection officer (DPO)	A, Chapter 2	Article 37, Article 38, Article 39	Subclause 6.3.1.1, Subclause 6.4.2.2, Subclause 6.10.2.4

4. Data protection impact assessment (DPIA)				
	4.1 Criteria for a data protection impact assessment (DPIA)	A, Chapter 5, Chapter 6, Chapter 7, Chapter 8	Article 35	Subclause 5.2.2, Subclause 7.2.5, Subclause 8.2.1
	4.2 Steps of a data protection impact assessment (DPIA)	A, Chapter 5, Chapter 7, Chapter 8	*no reference*	Subclause 5.2.2, Subclause 7.2.5, Subclause 8.2.1
5. Data breaches, notification, and incident response				
	5.1 GDPR requirements with regard to personal data breaches	A, Chapter 3, Chapter 14	Article 4(12), Article 33, Article 34	Subclause 6.13.1.1, Subclause 6.13.1.5
	5.2 Requirements for notification	A, Chapter 14	Article 33, Article 34	Subclause 6.13.1.1, Subclause 6.13.1.5

Contact EXIN

www.exin.com