Preparation Guide

Edition 201912

Content

1. Overview

EXIN Privacy & Data Protection Foundation (PDPF.EN)

Scope

EXIN Privacy & Data Protection Foundation (PDPF) is a certification that validates a professional's knowledge and understanding of the protection of personal data, the EU rules and regulations regarding data protection.

Summary

Wherever personal data is collected, stored, used, and finally deleted or destroyed, privacy concerns arise. With the EU General Data Protection Regulation (GDPR) the Council of the European Union aims to strengthen and unify data protection for all individuals within the European Union (EU). This regulation affects every organization that processes personal data of EU citizens. The EXIN Privacy & Data Protection Foundation certification covers the main subjects related to the GDPR.

The new 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 the new ISO standard helps fulfill the GDPR obligations to 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 literature, the GDPR and the ISO/IEC 27701:2019 standard to give the certification a broader context.

Context

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

Target Group

All employees who must have an understanding of data protection and European legal requirements as defined in the GDPR. This certification is tailored for:

- data protection officers (DPOs);
- compliance officers;
- security officers;
- HR staff;
- process and project managers.

Requirements for Certification

- Successful completion of the EXIN Privacy & Data Protection Foundation exam.

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	60 minutes

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

Bloom Level

The EXIN Privacy & Data Protection Foundation certification tests candidates at Bloom Level 1 and Level 2 according to Bloom's Revised Taxonomy:

- Bloom Level 1: Remembering – relies on recall of information. Candidates will need to absorb, remember, recognize and recall. This is the building block of learning before candidates can move on to higher levels.
- 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.

Training

Contact Hours

The recommended number of contact hours for this training course is 14. This includes group assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication Study Effort

60 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 Requirements	Exam Specifications	Weight
1. Privacy & Data Protection Fundamentals and Regulations		**47.5%**
	1.1 Definitions	7.5%
	1.2 Personal Data	17.5%
	1.3 Legitimate Grounds and Purpose Limitation	5%
	1.4 Further Requirements for Legitimate Processing of Personal Data	5%
	1.5 Rights of Data Subjects	2.5%
	1.6 Personal Data Breach and Related Procedures	10%
2. Organizing Data Protection		**35%**
	2.1 Importance of Data Protection for the Organization	12.5%
	2.2 Supervisory Authority[1]	7.5%
	2.3 Personal Data Transfer to Third Countries	7.5%
	2.4 Binding Corporate Rules and Data Protection in Contracts	7.5%
3. Practice of Data Protection		**17.5%**
	3.1 Data Protection by Design and by Default Related to Information Security	5%
	3.2 Data Protection Impact Assessment (DPIA)	5%
	3.3 Personal Data in Use	7.5%
	Total	**100%**

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

Exam Specifications

1 Privacy & Data Protection Fundamentals and Regulations

1.1 Definitions

The candidate can…

1.1.1 define privacy.

1.1.2 relate privacy to personal data and data protection.

1.1.3 describe the context of Union and Member state law.

1.2 Personal Data

The candidate can…

1.2.1 define personal data according to the GDPR.

1.2.2 make a distinction between personal data and special categories of data, like sensitive personal data.

1.2.3 describe the data subject's rights regarding personal data.

1.2.4 define processing of personal data that falls within the scope of the GDPR.

1.2.5 list the roles, responsibilities and stakeholders in the GDPR.

1.3 Legitimate Grounds and Purpose Limitation

The candidate can…

1.3.1 list the six legitimate grounds for processing.

1.3.2 describe the concept of purpose limitation.

1.3.3 describe proportionality and subsidiarity.

1.4 Further Requirements for Legitimate Processing of Personal Data

The candidate can…

1.4.1 describe the requirements for legitimate data processing.

1.4.2 describe the purpose of personal data processing.

1.4.3 explain the principles relating to processing of personal data.

1.5 Rights of Data Subjects

The candidate can…

1.5.1 describe the rights regarding data portability and the right of inspection.

1.5.2 describe the right to be forgotten.

1.6 Personal Data Breach and Related Procedures

The candidate can…

1.6.1 describe the concept of personal data breach.

1.6.2 explain procedures on how to act when a personal data breach occurs.

1.6.3 give examples of categories of personal data breaches.

1.6.4 describe the difference between a security breach (incident) and a personal data breach.

1.6.5 list relevant stakeholders that should be informed in case of a personal data breach.

2 Organizing Data Protection

2.1 Importance of Data Protection for the Organization

The candidate can…

2.1.1 list the different types of administration (GDPR Article 28 & Article 30).

2.1.2 indicate what activities are required to comply with the GDPR.

2.1.3 define data protection by design and by default.

2.1.4 give examples of personal data breaches.

2.1.5 describe the personal data breach notification obligation as laid down in the GDPR.

2.1.6 describe enforcement of the rules by issuing penalties including administrative fines.

2.2 Supervisory Authority
The candidate can…
2.2.1 describe the general responsibilities of a supervisory authority.
2.2.2 describe the role and responsibilities of a supervisory authority related to personal data breaches.
2.2.3 describe how a supervisory authority contributes to the application of the GDPR.

2.3 Personal Data Transfer to Third Countries
The candidate can…
2.3.1 describe the regulations that apply to data transfer inside the EEA.
2.3.2 describe the regulations that apply to data transfer outside the EEA.
2.3.3 describe the regulations that apply to data transfer between the EEA and the USA.

2.4 Binding Corporate Rules and Data Protection in Contracts
The candidate can…
2.4.1 describe the concept of binding corporate rules (BCR).
2.4.2 describe how data protection is formalized in contracts between the controller and the processor.
2.4.3 describe the clauses of such a contract.

3 Practice of Data Protection

3.1 Data Protection by Design and by Default
The candidate can…
3.1.1 describe the benefits of data protection by design and by default.
3.1.2 describe the seven principles of data protection by design.

3.2 Data Protection Impact Assessment (DPIA)
The candidate can…
3.2.1 outline what a DPIA covers and when to do a DPIA.
3.2.2 mention the eight objectives of a DPIA.
3.2.3 list the topics of a DPIA report.

3.3 Personal Data in Use
The candidate can…
3.3.1 describe the purpose of data lifecycle management (DLM).
3.3.2 explain data retention and minimization.
3.3.3 describe what a cookie is and what its purpose is.
3.3.4 describe the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

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
- authenticity
- availability
- awareness
- benchmark
- binding corporate rules (BCR)
- certification / certification bodies
- codes of conduct
- collecting personal data
- commission reports
- complaint
- compliance
- consent
  - child's consent
  - conditions for consent
  - explicit consent
- consistency / consistency mechanism
- constitution
- controller
- cross-border processing
- data accuracy
- data breach
- data classification system
- data concerning health
- data lifecycle management (DLM)
- data privacy breach response plan
- 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)
  - designation
  - position
  - tasks
- data subject
- data transfer
- declaration of consent
- delegated acts and implementing acts
  - committee procedure
- derogation
- documentation obligation
- enforcement
  - administrative fines
  - administrative penalties
  - criminal penalties
  - dissuasive penalties
  - effective penalties
  - proportionate penalties
- enterprise
- 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 Economic Area (EEA)
- European Union legal acts on data protection
- exchange of information
- exemption
- filing system
- General Data Protection Regulation (GDPR)
- governing body
- group of undertakings
- information society service
- international organization
- joint controllers
- judicial remedy
- lawfulness of processing
- legal basis
- 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
principles relating 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 officer / chief privacy officer
privacy by design (and by default)
processing (of personal data)
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
recipient
relevant and reasoned objection
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
- restrictions
- right to compensation
- right to objection
- transparency

rules of procedure
security breach
security incident
security of personal data
security of processing
sensitive data
seven principles for privacy by design
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

vulnerability

4. Literature

Exam Literature

The knowledge required for the exam is covered in the following literature:

A. L. Besemer
Whitepaper: EXIN Privacy & Data Protection Foundation
Free download on www.exin.com

Additional Literature

B. 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
Free download on: http://eur-lex.europa.eu (pdf) or https://gdpr-info.eu/ (html)

C. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

D. A. Calder
EU GDPR, A pocket guide
IT Governance Publishing
ISBN 978-1-84928-855-2 (paperback)
ISBN 978-1-84928-857-6 (e-book)

Comment

Additional literature is for reference and depth of knowledge only.

The GDPR text (source B) 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 exam literature.

Literature Matrix

Exam Requirements	Exam Specifications	Literature Reference	GDPR Reference	ISO/IEC 27701 Reference
1. Privacy & Data Protection Fundamentals and Regulations				
	1.1 Definitions	A, Chapter 1	Recital 1, 2 & Article 96-99	*no reference*
	1.2 Personal Data	A, Chapter 1, Chapter 2	Article 4.1(a), Article 9.1, Article 17, Article 4.10	Subclause 7.2.2, Subclause 7.3.6
	1.3 Legitimate Grounds and Purpose Limitation	A, Chapter 3	Article 6.1, Article 24	Subclause 7.2.2
	1.4 Further Requirements for Legitimate Processing of Personal Data	A, Chapter 3	Article 25, Article 27-32, Article 5	Subclause 5.2.1. *Article 5 is referenced throughout the standard*
	1.5 Rights of Data Subjects	A, Chapter 4	Article 15, Article 16, Article 17, Article 18, Article 20, Article 21, Article 22	Subclause 7.2.2, Subclause 7.3.2, Subclause 7.3.6, Subclause 7.3.9, Subclause 7.3.10, Subclause 7.5.1
	1.6 Personal Data Breach and Related Procedures	A, Chapter 5	Article 4(12), Article 33, Article 34	Subclause 6.13.1.5
2. Organizing Data Protection				
	2.1 Importance of Data Protection for the Organization	A, Chapter 2, Chapter 3, Chapter 5, Chapter 6, Chapter 7	Article 7, Article 8, Article 13, Article 25(1), Article 30, Article 83	Subclause 6.11.2.1, Subclause 6.11.2.5, Subclause 7.2.3, Subclause 7.2.4, Subclause 7.2.5, Subclause 7.2.8, Subclause 7.3.2, Subclause 7.3.6, Subclause 7.3.10, Subclause 7.5, Subclause 8.2.6, Subclause 8.5.2, Subclause 8.5.3
	2.2 Supervisory Authority	A, Chapter 7	Article 33, Article 34, Article 36	Subclause 5.2.2, Subclause 6.13.1.1, Subclause 6.13.1.5, Subclause 7.2.5
	2.3 Personal Data Transfer to Third Countries	A, Chapter 7	Article 29, Article 30, Article 45	Subclause 7.2.8, Subclause 7.5, Subclause 8.2.2, Subclause 8.2.6

	2.4 Binding Corporate Rules and Data Protection in Contracts	A, Chapter 7	Article 24, Article 28, Article 47	Subclause 5.2.1, Subclause 6.12.1.2, Subclause 7.2.6, Subclause 7.2.8, Subclause 7.5.1, Subclause 8.5
3. Practice of Data Protection				
	3.1 Data Protection by Design and by Default Related to Information Security	A, Chapter 7, Chapter 8	Article 25	Section B.8.4, Subclause 6.11.2.1, Subclause 6.11.2.5, Subclause 7.4.2
	3.2 Data Protection Impact Assessment (DPIA)	A, Chapter 8	Article 35	Subclause 5.2.2, Subclause 7.2.5, Subclause 8.2.1
	3.3 Practice-related Applications of the Use of Data, Marketing and Social Media	A, Chapter 4, Chapter 8	*no reference*	Section B.8.2.3

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER