Preparation Guide

Edition 201805

Content

1. Overview 4
2. Exam requirements 6
3. List of Basic Concepts 9
4. Literature 12

1. Overview

EXIN Privacy & Data Protection Foundation (PDPF.EN)

Scope

EXIN Privacy and Data Protection Foundation (PDPF) is a certification that validates a professional's knowledge about organizing 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 attempts to strengthen and unify data protection for all individuals within the European Union (EU). This regulation affects every organization that processes EU personal data. PDPF covers the main subjects related to the GDPR.

Context

The certificate EXIN Privacy and Data Protection Foundation (PDPF) is part of the EXIN qualification program Privacy and Data Protection.

Target group

All employees who need to have an understanding of data protection and European legal requirements as defined in the GDPR. More specific the following roles could be interested: Data Protection Officer, Privacy Officer, Legal Officer / Compliance Officer, Security Officer, Business Continuity Manager.

Requirements for certification

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

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40 questions
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Time allotted for examination:	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 15. This includes exam preparation and short breaks. This number of hours does not include homework, logistics for exam preparation and lunch breaks.

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 requirement	Exam specification	Weight
1. Privacy and Data Protection Fundamentals & Regulation		**44.5%**
	1.1 Definitions	7.5%
	1.2 Personal Data	12%
	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	5%
	1.6 Data Breach and Related Procedures	10%
2. Organizing Data Protection		**35.5%**
	2.1 Importance of Data Protection for the Organization	13%
	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		**20%**
	3.1 Data Protection by Design and by Default Related to Information Security	5%
	3.2 Data Protection Impact Assessment (DPIA)	5%
	3.3 Practice Related Applications of the Use of Data, Marketing and Social Media	10%
	Total	100%

[1] Before the GDPR was introduced the data protection authority was the national authority in charge with the enforcement of regulation on data protection. In the GDPR it is now called the supervisory authority.

Exam specifications

1 Privacy and Data Protection Fundamentals & Regulation

1.1 Definitions

The candidate can …

1.1.1 give valid definitions of privacy.

1.1.2 relate privacy, in specific personal data, to the concept of data protection.

1.1.3 describe the context of Union and Member state law.

1.2 Personal Data

The candidate can…

1.2.1 give a definition of personal data according to the GDPR.

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

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

1.2.4 describe processing of personal data.

1.2.5 list the roles, responsibilities and stakeholders.

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 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…

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

1.5.2 is aware of the right to be forgotten.

1.6 Data Breach and Related Procedures

The candidate can…

1.6.1 describe the concept of data breach.

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

1.6.3 give examples of categories of data breaches.

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

1.6.5 mention relevant stakeholders that should be informed.

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 art 28 & 30).
2.1.2 indicate what activities are required to comply with the GDPR.
2.1.3 give a definition of data protection by design and by default.
2.1.4 give examples of data breaches.
2.1.5 describe the 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 responsibility of a supervisory authority related to 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 written contracts between the controller and the processor.
2.4.3 describe the clauses of such a written contract.

3 Practice of Data Protection

3.1 Data protection by design and data protection by default

The candidate can…

3.1.1 describe the benefits of the application of the principles 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 comprises and when to apply a DPIA.
3.2.2 mention the eight objectives of a DPIA.
3.2.3 list the topics of a DPIA report.

3.3 Practice Related Applications of the Use of Data, Marketing and Social Media

The candidate can…

3.3.1 describe the purpose of Data Life Cycle (DLC) management.
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, from a data protection perspective, how the wide spread use of internet has affected the field of marketing.
3.3.5 give examples of how social media information is used for Marketing activities.

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
- binding
- binding corporate rules
- biometric data
- certification
- certification bodies
- child's consent
- 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 breach
- data concerning health
- data controller
- data protection
- data protection authority
- data protection by default
- data protection by design
- data protection impact assessment
- data protection officer (DPO)
  - designation
  - position
  - tasks
- data subject
- data transfer
- delegated acts and implementing acts
  - committee procedure
- 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
- genetic data
- filing system
- General Data Protection Regulation (GDPR)
- governing body
- group of undertakings
- independent supervisory authorities
  - activity reports
  - competence
  - establishment
  - powers
  - tasks
- information society service
- international organization
- joint controllers
- judicial remedy
- lawfulness of processing
- legal basis
- legitimate ground (GDPR article 17/1c, article 18/1d, article 21/1) and legitimate basis (GDPR article 40)
- legitimate interest
- liability
- main establishment
- material scope
- National Identification Number
- non-repudiation
- opinion of the board
- personal data
- personal data breach
- personal data relating to criminal convictions and offences
- principles relating to processing of personal data
  - accountability
  - accuracy
  - confidentiality
  - data minimization
  - fairness
  - integrity
  - lawfulness
  - purpose limitation
  - storage limitation
  - transparency
- prior consultation
- privacy
- processing
- 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

pseudonymization

recipient

relevant and reasoned objection

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

rules of procedure

security breach (security incident)

security of personal data

security of processing

sensitive data

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

supervisory authority

supervisory authority concerned

suspension of proceedings

territorial scope

third party

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

4. Literature

Exam literature

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

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

B. L. Besemer
White Paper – EXIN Privacy and Data Protection Foundation
Free download on www.exin.com

C. European Commision
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

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 matrix

Exam requirement	Exam specification	Literature	GDPR reference
1. Privacy and Data Protection Fundamentals & Regulation			
	1.1 Definitions	A: Ch. 1, Ch. 3 B: §1.1.1	rec. 1, 2 & art 96-99
	1.2 Personal Data	A: Ch. 2, Ch. 3 B: §1.1.3, §1.3.6, §1.3.7, §4	art. 4.1 (a), art 9.1, art 17, art 4.10
	1.3 Legitimate Grounds and Purpose Limitation	B: §3.1, §3.2, §3.3	art 6.1, art 24
	1.4 Further Requirements for Legitimate Processing of Personal Data	B: §2.1, §6.1	art 25, art 27-32, art 5
	1.5 Rights of Data Subjects	B: §4.3, §4.4.2	no ref.
	1.6 Data Breach and Related Procedures	B: §5.1-5.3	art 4(12), art 33, art 34
2. Organizing Data Protection			
	2.1 Importance of Data Protection for the Organization	A: Ch. 3, Ch. 4 B: §5.2, §5.3, §6.1, §6.3, §8.1	art 7, art 8, art 13, art 30, art 25(1), art 83
	2.2 Supervisory Authority	A: Ch. 3 B: §7.1, §7.3	art 36, art 33, art 34
	2.3 Personal Data Transfer to Third Countries	B: §7.4	art 29, art 30, art 45
	2.4 Binding Corporate Rules and Data Protection in Contracts	A: Ch. 3 B: §7.4.3.3, §8.2	art 47, art 24, art 28
3. Practice of Data Protection			
	3.1 Data Protection by Design and by Default Related to Information Security	B: §5.2, §8.1.1	no ref.
	3.2 Data Protection Impact Assessment (DPIA)	§6.1.3, §8.3, §8.5	no ref.
	3.3 Practice Related Applications of the Use of Data, Marketing and Social Media	§8.4, §8.6	no ref.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER