Preparation Guide

Edition 202508

Content

1. Overview

EXIN Privacy & Data Protection Foundation (PDPF.EN)

Scope

The EXIN Privacy & Data Protection Foundation certification confirms that the professional understands the basic concepts and principles of data protection in the context of the General Data Protection Regulation (GDPR).

This certification includes the following topics:

- GDPR scope
- Principles of data processing
- Practice of data processing
- International personal data transfers
- Risk assessment and mitigation

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.

With the enormous increase in use of artificial intelligence (AI), there is more demand for the use of personal data to train the algorithms. This poses new challenges for data protection that must be addressed properly for compliance with the GDPR.

The relevant 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 to:

- 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% (26/40)
Open book:	No
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

56 hours (2 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. GDPR scope		**12.5%**
	1.1 Privacy and data protection	5%
	1.2 Scope of the GDPR	7.5%
2. Principles of data processing		**37.5%**
	2.1 Stakeholder roles, rights, and obligations	7.5%
	2.2 Data protection by design and by default	5%
	2.3 Legitimate grounds for processing	5%
	2.4 Rights of the data subjects	12.5%
	2.5 Principles of processing personal data	7.5%
3. Practice of data processing		**10%**
	3.1 Data governance	2.5%
	3.2 Processing online	2.5%
	3.3 Using artificial intelligence (AI)	5%
4. International personal data transfers		**15%**
	4.1 Cross-border transfers within the European Economic Area (EEA)	10%
	4.2 Cross-border transfers outside the European Economic Area (EEA)	5%
5. Risk assessment and mitigation		**25%**
	5.1 Data protection impact assessment (DPIA) and prior consultation	7.5%
	5.2 Personal data breaches and related procedures	12.5%
	5.3 Supervisory authorities	5%
	Total	**100%**

Exam specifications

1 GDPR scope

1.1 Privacy and data protection

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 European Union (EU) and EU Member State law.

1.2 Scope of the GDPR

The candidate can…

1.2.1 define personal data according to the GDPR.

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

1.2.3 make a distinction between personal data and special categories of data.

2 Principles of data processing

2.1 Stakeholder roles, rights, and obligations

The candidate can…

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

2.1.2 describe the process and activities required to comply with the GDPR.

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

2.2 Data protection by design and by default

The candidate can…

2.2.1 describe the seven principles of data protection by design.

2.2.2 describe the benefits of data protection by design and by default.

2.3 Legitimate grounds for processing

The candidate can…

2.3.1 list the six legitimate grounds for processing.

2.3.2 describe the requirements for lawful data processing.

2.4 Rights of the data subjects

The candidate can…

2.4.1 describe the right to transparent information, communication, and modalities.

2.4.2 describe the right of access.

2.4.3 describe the right to data portability.

2.4.4 describe the right to rectification.

2.4.5 describe the right to erasure.

2.4.6 describe the right to restriction of processing.

2.4.7 describe the right to object and the right to lodge a complaint with the supervisory authority.

2.4.8 describe rights regarding automated decision-making.

2.5 Principles of processing personal data

The candidate can…

2.5.1 describe lawfulness, fairness, and transparency.

2.5.2 describe purpose specification and purpose limitation.

2.5.3 describe data minimization and storage limitation.

2.5.4 describe accuracy, integrity, and confidentiality of personal data.

2.5.5 describe proportionality and subsidiarity.

3 Practice of data processing

3.1 Data governance

The candidate can…

3.1.1 describe the purpose of data lifecycle management (DLM).

3.2 Processing online

The candidate can…

3.2.1 describe the definition, functionality, and purpose of a cookie.

3.2.2 describe the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

3.3 Using artificial intelligence (AI)

The candidate can…

3.3.1 identify challenges to GDPR compliance when using AI.

3.3.2 describe conditions for compliance with the GDPR when using AI.

4 International personal data transfers

4.1 Cross-border transfers within the European Economic Area (EEA)

The candidate can…

4.1.1 describe the regulations that apply to data transfers inside the EEA.

4.1.2 describe the concept of binding corporate rules (BCR).

4.1.3 describe how data protection is formalized in BCR between the controller and the processor.

4.1.4 describe the clauses of BCR.

4.2 Cross-border transfers outside the European Economic Area (EEA)

The candidate can…

4.2.1 describe the regulations that apply to data transfers outside the EEA.

4.2.2 describe the regulations that apply to data transfers between the EEA and the United States of America (U.S.)

5 Risk assessment and mitigation

5.1 Data protection impact assessment (DPIA) and prior consultation

The candidate can…

5.1.1 outline what a DPIA covers and when to do a DPIA.

5.1.2 list the eight objectives of a DPIA.

5.1.3 list the topics of a DPIA report.

5.2 Personal data breaches and related procedures

The candidate can…

5.2.1 define a personal data breach.

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

5.2.3 give examples of personal data breaches.

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

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

5.3 Supervisory authorities

The candidate can…

5.3.1 describe the general responsibilities of a supervisory authority.

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

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
artificial intelligence (AI)
awareness
certification
codes of conduct
complaint
compliance audit
consent
- child's consent
- conditions for consent
- explicit consent

constitution
cross-border processing
data breach
data lifecycle management (DLM)
data protection
data protection authority (DPA)
data protection by default
data protection by design
data protection impact assessment (DPIA)
data protection officer (DPO)
derogation
documentation obligation
enforcement
- administrative fines
- criminal sanctions
- dissuasive sanctions
- effective sanctions
- proportionate sanctions

European Union (EU) types of legal act
- decision
- directive
- opinion
- recommendation
- regulation

European Data Protection Board (EDPB)
European Data Protection Supervisor (EDPS)
European Economic Area (EEA)
exemption
GDPR (General Data Protection Regulation)
information security (InfoSec)
- availability
- confidentiality
- integrity

international organization
lead data protection authority
lead supervisory authority
legitimate basis (GDPR Recital 40)
legitimate ground (GDPR Article 17(1c), Article 18(1d), Article 21(1))
legitimate interest
non-repudiation
personal data
personal data breach
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 by design (and by default)
processing (of personal data)
- collection
- storage
- erasure
- destruction

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

profiling
proportionality, the principle of
pseudonymization
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

roles, responsibilities, and stakeholders
- controller
- data subject
- joint controllers
- processor
- recipient
- representative
- supervisory authority
- third party

security breach
security incident
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
- personal data relating to criminal convictions and offences

subsidiarity, the principle of
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

4. Literature

Exam literature

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

A. L. Besemer
Privacy and Data Protection based on the GDPR (second edition)
Leo Besemer, 2025
ISBN: 9789403795751
Hard copy: https://publishnl.bookmundo.com/leobesemer
E-book: https://www.kobo.com/nl/en/ebook/privacy-and-data-protection-based-on-the-gdpr-3

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: https://eur-lex.europa.eu/eli/reg/2016/679

C. A. Cavoukian
Privacy by Design - The 7 Foundational Principles
Information & Privacy Commissioner, Ontario, Canada
https://bit.ly/pdpf_additional_literature

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		References		
	Exam specifications	**Literature**	**GDPR**	**ISO/IEC 27701**
1. GDPR scope				
	1.1 Privacy and data protection	A, Chapter 1	Recital 1, 2, Article 96-99	*no reference*
	1.2 Scope of the GDPR	A, Chapter 1	Article 4.1(a), Article 9.1, Article 17, Article 4.10	Subclause 7.2.2, Subclause 7.3.6
2. Principles of data processing				
	2.1 Stakeholder roles, rights, and obligations	A, Chapter 2	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 Data protection by design and by default	A, Chapter 2	Article 25	Section B.8.4, Subclause 6.11.2.1, Subclause 6.11.2.5, Subclause 7.4.2
	2.3 Legitimate grounds for processing	A, Chapter 4	Article 6.1	Subclause 7.2.2, Subclause 5.2.1
	2.4 Rights of the data subjects	A, Chapter 5	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
	2.5 Principles of processing personal data	A, Chapter 3	Article 25, Article 27-32, Article 5	Subclause 5.2.1., entire standard
3. Practice of data processing				
	3.1 Data governance	A, Chapter 6	*no reference*	Section B.8.2.3
	3.2 Processing online	A, Chapter 7	*no reference*	*no reference*
	3.3 Using artificial intelligence (AI)	A, Chapter 7	*no reference*	*no reference*
4. International personal data transfers				
	4.1 Cross-border transfers within the European Economic Area (EEA)	A, Chapter 8	Article 29, Article 30, 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, Subclause 8.5
	4.2 Cross-border transfers outside the European Economic Area (EEA)	A, Chapter 9	Article 45	Subclause 8.2.2, Subclause 8.2.6

5. Risk assessment and mitigation				
	5.1 Data protection impact assessment (DPIA) and prior consultation	A, Chapter 10	Article 35	Subclause 5.2.2, Subclause 7.2.5, Subclause 8.2.1
	5.2 Personal data breaches and related procedures	A, Chapter 11	Article 4(12), Article 33, Article 34	Subclause 6.13.1.5
	5.3 Supervisory authorities	A, Chapter 12	Article 33, Article 34, Article 36	Subclause 5.2.2, Subclause 6.13.1.1, Subclause 6.13.1.5, Subclause 7.2.5

5. Career Path

At EXIN, we believe in the value of lifelong learning and the importance of combining diverse skills to thrive in today's dynamic and evolving world. With our EXIN Career Paths, candidates can prepare for specific job roles and continue to grow and advance in their professional journey. For more information on EXIN Career Paths, please refer to https://www.exin.com/career-paths/.

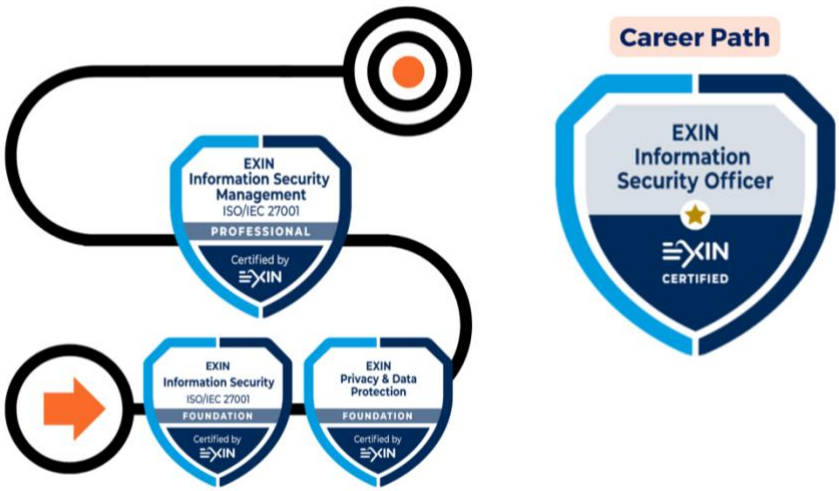
The EXIN Privacy & Data Protection Foundation certification is part of the following EXIN Career Paths.

EXIN Data Protection Officer

EXIN Data Protection Officer enables professionals to implement measures for information security management that are aimed at complying with data protection regulations.

EXIN Information Security Officer

EXIN Information Security Officer equips professionals with knowledge and skills to implement effective information security measures and risk management, while keeping a focus on data protection and privacy.



EXIN Artificial Intelligence Compliance Officer

EXIN Artificial Intelligence Compliance Officer prepares professionals to comply with the most relevant artificial intelligence (AI) and data protection regulations, and robust information security standards, to ensure ethical and responsible use of AI.

Contact EXIN

www.exin.com