



Preparation Guide

Edition 201810

Copyright © EXIN Holding B.V. 2018. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.



Content

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

1. Overview

EXIN Privacy & Data Protection Essentials (PDPE.EN)

Scope

EXIN Privacy and Data Protection Essentials (PDPE) 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 EXIN Privacy & Data Protection Essentials (PDPE) is part of the EXIN qualification program Privacy and Data Protection. The Essentials exam is a subset of the Foundation exam. It cannot be used to gain access to the Practitioner exam, but is meant for those that need a basic understanding of the GDPR.



Target group

Everyone that wants or needs to have a basic understanding of data protection and European legal requirements as defined in the GDPR. The Essentials exam is exceptionally suitable for everyone that needs to make informed decisions regarding the privacy and data protection of their own data.

Requirements for certification

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

Examination details

Examination type:	Multiple-choice questions
Number of questions:	20 questions
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Time allotted for examination:	30 minutes

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

Bloom level

The EXIN Privacy & Data Protection Essentials 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.

Training

Contact hours

The recommended number of contact hours for this training course is 7. This includes group assignments, exam preparation and short breaks. This number of hours does not include homework, the exam session and lunch breaks.

Indication study effort

20 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		50%
	1.1 Definitions	10%
	1.2 Personal data	15%
	1.3 Legitimate grounds and purpose limitation	10%
	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	5%
2. Organizing data protection		25%
	2.1 Importance of data protection for the organization	10%
	2.2 Supervisory authority ¹	5%
	2.3 <i>Personal data transfer to third countries</i> ²	--
	2.4 Binding Corporate rules and data protection in contracts	10%
3. Practice of data protection		25%
	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	15%
	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*.

² Exam specification 2.3 is only tested in the EXIN Privacy and Data Protection Foundation exam

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.

1.2 Personal Data

The candidate can ...

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

1.2.3 describe the data subject's rights regarding 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.

1.5 Rights of Data Subjects

The candidate can ...

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.

2 Organizing data protection

2.1 Importance of Data Protection for the Organization

The candidate can ...

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.

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

2.2 Supervisory Authority

The candidate can ...

2.2.1 describe the general responsibilities of a supervisory authority.

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.

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.

3.2 Data Protection Impact Assessment (DPIA)

The candidate can ...

3.2.1 outline what a DPIA comprises and when to apply a DPIA.

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.

3.3.3 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. 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	cross-border processing
appropriate technical and organizational measures	data breach
authenticity	data concerning health
availability	data controller
binding	data protection
binding corporate rules	data protection authority
biometric data	data protection by default
certification	data protection by design
certification bodies	data protection impact assessment
child's consent	data protection officer (DPO) <ul style="list-style-type: none">• designation• position• tasks
codes of conduct	data subject
collection of personal data (verb.)	data transfer
commission reports	delegated acts and implementing acts <ul style="list-style-type: none">• committee procedure
complaint	derogation
compliance	enforcement <ul style="list-style-type: none">• administrative fines• administrative penalties• criminal penalties• dissuasive penalties• effective penalties• proportionate penalties
conditions for consent	enterprise
consent	European Economic Area (EEA)
consistency	EU types of legal act <ul style="list-style-type: none">• decision• directive• opinion• recommendation• regulation
consistency mechanism	
constitution	
contract	
controller	

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	security of personal data
pseudonymization	security of processing
recipient	sensitive data
relevant and reasoned objection	special categories of personal data
	<ul style="list-style-type: none">• 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
representative	supervisory authority
restriction of processing	supervisory authority concerned
retention period	suspension of proceedings
right to compensation	territorial scope
rights of the data subject	third party
<ul style="list-style-type: none">• 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	transfer of personal data to third countries and to international organizations
	<ul style="list-style-type: none">• adequacy decision• appropriate safeguards• binding corporate rules• derogations• disclosures• international protection of personal data
security breach (security incident)	

4. Literature

Exam literature

The knowledge required for the EXIN Privacy & Data Protection Essentials 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 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>

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
	2.4 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

