

COURSEWARE

Privacy & Data Protection Foundation

Courseware - English



Auteur: Ruben Zeegers



Privacy & Data Protection
Foundation Courseware – English

Colofon

Title: Privacy & Data Protection Foundation Courseware – English

Authors: Ing. Ruben Zeegers CISSP RSE

Publisher: Van Haren Publishing, 's-Hertogenbosch

ISBN Hard Copy: 978 94 018 035 95

Edition: First edition, first print October 2018

Design: Van Haren Publishing, 's-Hertogenbosch

Copyright: © Van Haren Publishing 2018

For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

All rights reserved. No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by the publisher.

Although this publication has been composed with much care, neither author, nor editor, nor publisher can accept any liability for damage caused by possible errors and/or incompleteness in this publication.

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

About the Courseware

The Courseware was created by experts from the industry who served as the author(s) for this publication. The input for the material was based on existing publications and the experience and expertise of the author(s). The material has been revised by trainers who also have experience working with the material. Close attention was also paid to the key learning points to ensure what needs to be mastered.

The objective of the courseware is to provide maximum support to the trainer and to the student, during his or her training. The material has a modular structure and according to the author(s) has the highest success rate should the student opt for examination. For this reason, the Courseware has also been accredited, wherever applicable.

In order to satisfy the requirements for accreditation the material must meet certain quality standards. The structure, the use of certain terms, diagrams and references are all part of this accreditation. Additionally, the material must be made available to each student in order to obtain full accreditation. To optimally support the trainer and the participant of the training assignments, practice exams and results have been provided with the material.

Direct reference to advised literature is also regularly covered in the sheets so that students can easily find additional information concerning a particular topic. The decision to separate note pages (handouts) from the Courseware was to encourage students to take notes throughout the material.

Although the courseware is complete, the possibility that the trainer may deviate from the structure of the sheets or chooses to not refer to all the sheets or commands does exist. The student always has the possibility to cover these topics and go through them on their own time. It is strongly recommended to follow the structure of the courseware and publications for maximum exam preparation.

The courseware and the recommended literature are the perfect combination to learn and understand the theory.

- Van Haren Publishing

Table of content

	<i>--- Slide number</i>	<i>--- Page number</i>
Reflection		7
Agenda		9
Course		11
About this Courseware	2	12
ISFS exam specifications	10	15
Module 1: Privacy & data protection fundamentals & regulation	13	17
1.1 Concepts in a digital world	14	17
1.2 Personal data	29	25
1.3 Legitimate grounds and purpose limitation	42	31
1.4 Further requirements for legitimate processing of personal data	55	38
1.5 Rights of data subjects	61	41
1.6 Data breach and related procedures	69	45
Module 2: Organizing data protection	79	50
2.1 The importance of data protection for the organization	80	51
2.2 Supervisory authority	100	60
2.3 Transfer of personal data to third countries	105	63
2.4 Binding Corporate rules and data protection in contracts	112	66
Module 3: Practice of data protection	126	73
3.1 Data protection by design and by default related to information security	127	74
3.2 Data protection impact assessment (DPIA)	143	82
3.3 Practice related applications of the use of data, marketing and social media.	155	88

Practice questions		
Questions Module 1	167	95
Questions Module 2	173	98
Questions Module 3	176	99
Assignment answers		
Answer Module 1	180	101
Answer Module 2	185	104
Answer Module 3	188	105
EXIN Sample Exam		107
Rationale		109
Answers		119
Evaluation		139
EXIN Preparation Guide		141
White paper Privacy and Data Protection Foundation		157

Self-Reflection of understanding Diagram

‘What you do not measure, you cannot control.’ – Tom Peters

Fill in this diagram to self-evaluate your understanding of the material. This is an evaluation of how well you know the material and how well you understand it. In order to pass the exam successfully you should be aiming to reach the higher end of Level 3. If you really want to become a pro, then you should be aiming for Level 4. Your overall level of understanding will naturally follow the learning curve. So, it’s important to keep track of where you are at each point of the training and address any areas of difficulty.

Based on where you are within the Self-Reflection of Understanding diagram you can evaluate the progress of your own training.

<i>Level of Understanding</i>	<i>Before Training (Pre-knowledge)</i>	<i>Training Part 1 (1st Half)</i>	<i>Training Part 2 (2nd Half)</i>	<i>After studying / reading the book</i>	<i>After exercises and the Practice exam</i>
<i>Level 4 I can explain the content and apply it .</i>					
<i>Level 3 I get it! I am right where I am supposed to be.</i>					Ready for the exam!
<i>Level 2 I almost have it but could use more practice.</i>					
<i>Level 1 I am learning but don't quite get it yet.</i>					

(Self-Reflection of Understanding Diagram)

Write down the problem areas that you are still having difficulty with so that you can consolidate them yourself, or with your trainer. After you have had a look at these, then you should evaluate to see if you now have a better understanding of where you actually are on the learning curve.

Troubleshooting

Problem areas:

Topic:

Part 1

Part 2

You have gone through the book and studied.

You have answered the questions and done the practice exam.

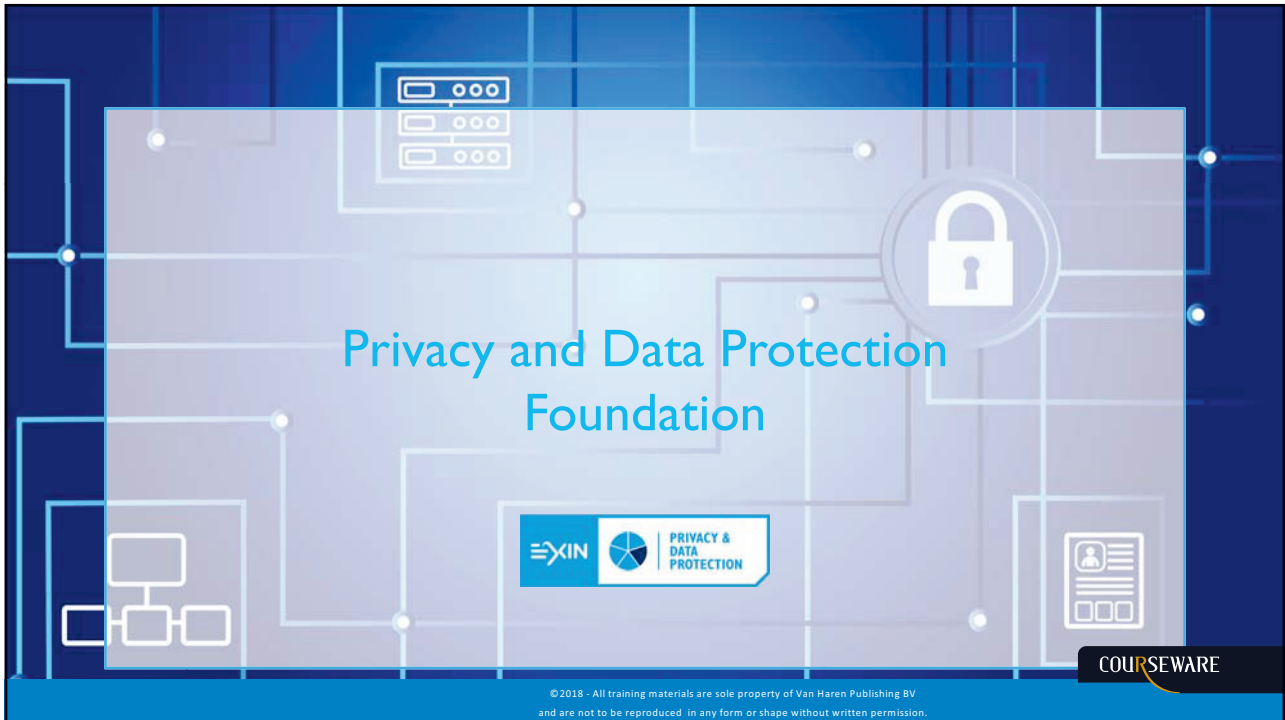
Timetable

Day 1

09:00 - 9:30	Introduction, About this course
09:30 - 12:00	Module 1: Privacy & data protection fundamentals & regulation
12:30 - 12:30	lunch
12:30 - 17:00	Module 2: Organizing data protection

Day 2

09:00 - 12:00	Module 3: Practice of data protection
12:00- 12:30	lunch
12:30 - 14:00	Practice questions & Evaluate
14:00 - 17:00	Sample Exam questions



The slide features a dark blue background with a light blue grid and circuit-like lines. In the center, the text "Privacy and Data Protection Foundation" is displayed in a light blue font. To the right of the text is a white padlock icon inside a circular frame. Below the text is a logo for "EXIN PRIVACY & DATA PROTECTION". In the bottom right corner, there is a "COURSEWARE" logo. At the very bottom, a small copyright notice reads: "© 2018 - All training materials are sole property of Van Haren Publishing BV and are not to be reproduced in any form or shape without written permission."

Privacy and Data Protection Foundation

EXIN PRIVACY & DATA PROTECTION

COURSEWARE


© 2018 - All training materials are sole property of Van Haren Publishing BV and are not to be reproduced in any form or shape without written permission.



The slide has a white background with a blue border. The title "Introduction" is centered at the top in a blue font. Below the title is a bulleted list with three items: "Let's meet & Goals", "Terms", and "Program". At the bottom center is a blue icon of two hands shaking. The footer contains the text "© Van Haren Publishing" on the left and the number "2" on the right.

Introduction

- Let's meet & Goals
- Terms
- Program



© Van Haren Publishing 2



Program

Privacy and Data Protection Foudation

Day 1

09:00 - 9:30	Introduction, About this course
09:30 - 12:00	Module 1: Privacy & data protection fundamentals & regulation
12:00 - 12:30	lunch
12:30 - 17:00	Module 2: Organizing data protection

Day 2

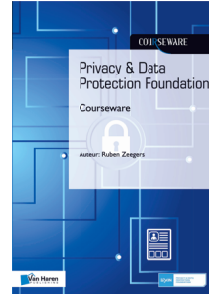
09:00 - 12:00	Module 3: Practice of data protection
12:00- 12:30	lunch
12:30 - 14:00	Practice questions & Evaluate
14:00 - 17:00	Sample Exam questions and review

Literature

Calder
EU GDPR, A pocket guide
IT Governance Publishing



White paper



Courseware



Trainer slides
(Included in Courseware)

Study book



Certification levels



Basic Concepts

- The list of Basic Concepts in the student notes below will be considered understood for the exam
- The student is advised to research and understand the concepts

Value of this certification

- EXIN Privacy and Data Protection Foundation (PDPF) is a certification that validates a professional's knowledge about data privacy and EU rules and regulations regarding data protection.
- Wherever personal data is collected, stored, used, and finally deleted or destroyed, privacy concerns rise. The EU General Data Protection Regulation (GDPR) affects every organization that processes EU personal data. PDPF covers the main subjects related to this regulation on data protection.

Course objectives and Target audience

After completing this course the participant will

- Be familiar with European legislation, regulations and directives
- Be familiar with privacy issues that may arise in their own organization
- Know how to formulate advise to help solve privacy issues

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.

Exam requirements

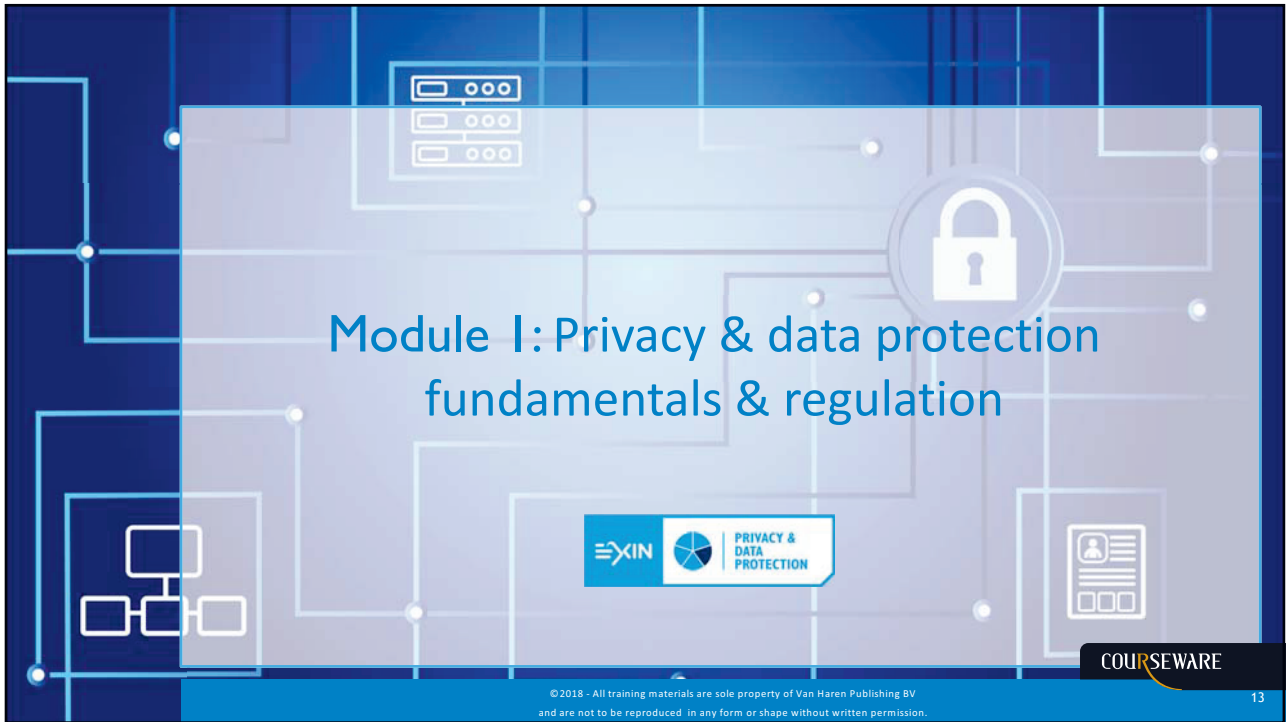
Exam requirement	Exam specification	Weight %
1. Privacy and data protection fundamentals & regulation		45
	1.1 Definitions	
	1.2 Personal data	
	1.3 Legitimate grounds and purpose limitation	
	1.4 Further requirements for legitimate processing of personal data	
	1.5 Rights of data subjects	
	1.6 Data breach and related procedures	
2. Organizing data protection		35
	2.1 Importance of data protection for the organization	
	2.2 Supervisory authority ¹	
	2.3 Personal data transfer to third countries	
	2.4 Binding Corporate rules and data protection in contracts	
3. Practice of data protection		20
	3.1 Data protection by design and by default related to information security	
	3.2 Data protection impact assessment (DPIA)	
	3.3 Practice related applications of the use of data, marketing and social media	
	Total	100%

Exam specifications

- Examination type: Computer-based or paper-based multiple-choice questions
- Number of questions: 40
- Pass mark: 65%
- Open book/notes: No
- Electronic equipment/aides permitted: No
- Time allotted for examination: 60 minutes



- 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>



Module I: Privacy & data protection
fundamentals & regulation

EXIN PRIVACY & DATA PROTECTION

COURSEWARE

© 2018 - All training materials are sole property of Van Haren Publishing BV and are not to be reproduced in any form or shape without written permission.

13

This slide features a dark blue background with a light blue grid and circuit-like lines. A central white padlock icon is prominent. The text is in a clean, sans-serif font. Logos for EXIN and COURSEWARE are positioned at the bottom. A small copyright notice is located at the very bottom center.



1.1 CONCEPTS IN A DIGITAL WORLD

© Van Haren Publishing

14

This slide has a dark, blurred background showing computer code and data visualizations. A semi-transparent white box at the bottom contains the title text. The EXIN logo is visible in the bottom right corner.

Definitions

Privacy

The right to respect for a person's private and family life, his or her home and correspondence.

Data Protection

From the former paragraphs, we can conclude that the GDPR is about the protection of personal data, not all data.

The history of data protection regulations

Quote:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... **the right 'to be let alone'** ... Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'

Louis D. Brandeis, Harvard Law Review, **1890**

Quote:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

article 12 of the Universal Declaration of Human Rights (UHDR), **1948**

Rapid progress in data processing

- The increased possibilities in the use of telecommunications in the 1970s coincided with the development of the European Union, Which increased trans-border trade.
- A need was felt for new standards that would allow individuals to exercise control over their personal information.
- International trade needed free international flow of information.
- The challenge was (and is) to find a balance between concerns for the protection of personal freedoms and the possibility to support free trade throughout Europe.

European Convention of Human Rights (ECHR)

- One of the first legal protections for personal information was codified in Article 8 of the European Convention on Human Rights (ECHR) in 1953.
- Provides the foundation for modern European privacy laws
- Article 8 reads:
 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

EU definitions of privacy

“Everyone has the right to the protection of personal data concerning them.”

- Treaty on the Functioning of Europe (‘Treaty of Rome 1957’)

“Everyone has the right to the protection of personal data concerning him or her.”

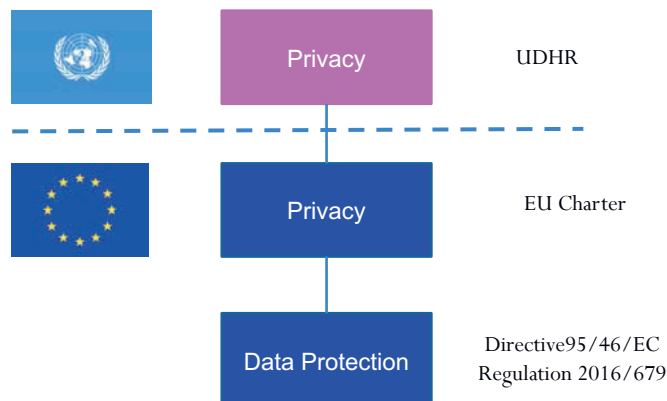
- Charter of Fundamental Rights of the European Union (2000)

First recital of the General Data Protection Regulation (GDPR)

- The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and
- Article 16 of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

EU and member state laws

The broader picture



Directive 95/46/EC & Regulation 2016/679

The **Data Protection Directive** 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (adopted in 1995). It regulates the processing of personal data within the European Union.

- *Directive 95/46/EC was repealed when the GDPR applied*

The **General Data Protection Regulation** (GDPR) 2016/679 is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU).

The Data Protection Directive (& GDPR) applies to countries of the **European Economic Area** (EEA).

- *This includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein and Norway. (EEA EFTA)*

Related EU legislation

Regulation 45/2001 (processing of personal data by the Community institutions and bodies and on the free movement of such data)

Directive 2002/58/EC (on privacy and electronic communications)

Directive 2016/680 (police and judicial cooperation in criminal matters)

Directive 2016/681 (on the use of passenger name record (PNR) data)

Decision 2001/497/EC (On standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC)

Decision No 1247/2002/EC (on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties)

Decision 2004/915/EC (Amending Decision 2001/497/EC...alternative set of standard contractual clauses)

Decision 2008/597/EC (rules concerning the Data Protection Officer)

Member state laws

Example:

- **Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application.**

Other national laws:

- **constitution**
- **civil code**
- **Police law**
- **Tax law**
- **Archives & records act**
- **Telecommunications act**
- **Etc.**

General Data Protection Regulation (GDPR)

The GDPR:

- Was adopted by the EU Council and Parliament in April 2016
- Went into effect in every EU member state on May 25th 2018
- Sets out requirements for organisations and for Member States
- Makes provision for the creation of an EU Data Protection Board

GDPR Infringements

- Organisations will not be fined without any form of process
- Failure to meet the requirements of the Regulation could be expensive
- The intent is that fines should be sufficiently substantial and painful to discourage breaches of the regulation
- The threat of such fines should, ideally, ensure that all data controllers and data processors will comply with the GDPR.

GDPR Penalties

- Infringements of some GDPR Articles carry the maximum administrative penalty:
4 percent of annual global turnover
or
€20 million
whichever is greater
- Infringements of the requirements in relation to international transfers are also subject to this higher penalty.

GDPR High Penalty Articles

- 5 - Principles relating to processing of personal data
- 6 - Lawfulness of processing
- 7 - Conditions for consent
- 9 - Processing of special categories of personal data
- 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject
- 13 - Information to be provided where personal data are collected from the data subject
- 14 - Information to be provided where personal data have not been obtained from the data subject
- 15 - Right of access by the data subject
- 16 - Right to rectification
- 17 - Right to erasure ('right to be forgotten')
- 18 - Right to restriction of processing
- 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing
- 20 - Right to data portability
- 21 - Right to object
- 22 - Automated individual decision-making, including profiling

Principles for Processing Personal Data

GDPR Article 5:

Six principles that should be applied to any activity that involves the collection or processing of personal data.

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to what is necessary for processing.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
6. Personal data must be processed in a manner that ensures its security.