COURSEWARE

Privacy & Data Protection Essentials

Courseware - English

Ruben Zeegers & Theo Wanders

EXIN Privacy & Data Protection ESSENTIALS Certified by EXIN

Van Haren PUBLISHING

Privacy & Data Protection
Essentials Courseware – English

Colofon

Title:	Privacy & Data Protection Essentials Courseware – English
Authors:	Ing. Ruben Zeegers CISSP RSE; Ing. Theo Wanders
Publisher:	Van Haren Publishing, 's-Hertogenbosch
ISBN Hard Copy:	978 940 180 457 8
Edition:	First edition, first print April 15 2019
Design:	Van Haren Publishing, 's-Hertogenbosch
Copyright:	© Van Haren Publishing 2019

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

The certificate EXIN Privacy and Data Protection Essentials (PDPE) 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

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Topics are (per domain):

IT and IT Management

ABC of ICT
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture

ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management

BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

Project Management

A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Table of content

	--- Slide number	--- Page number
Reflection		7
Agenda		9
Course		10
About this Courseware	3	11
PDPE exam specifications	10	14
Module 1: Privacy & data protection fundamentals & regulation	13	16
1.1 Concepts in a digital world	14	16
1.2 Personal data	26	22
1.3 Legitimate grounds and purpose limitation	33	26
1.4 Further requirements for legitimate processing of personal data	46	32
1.5 Rights of data subjects	49	34
1.6 Data breach and related procedures	56	37
Module 2: Organizing data protection	62	40
2.1 The importance of data protection for the organization	63	41
2.2 Supervisory authority	76	47
2.4 Binding Corporate rules and data protection in contracts	80	49
Module 3: Practice of data protection	88	53
3.1 Data protection by design and by default related to information security	89	54
3.2 Data protection impact assessment (DPIA)	94	56
3.3 Practice related applications of the use of data, marketing and social media.	104	61

Practice questions

Questions Module I	108	63
Questions Module 2	113	66
Questions Module 3	115	67

Assignment answers

Answer Module I	117	68
Answer Module 2	121	70
Answer Module 3	123	71

EXIN Preparation Guide 72

EXIN Sample Exam

Questions	85
Rational	90
Answers	100

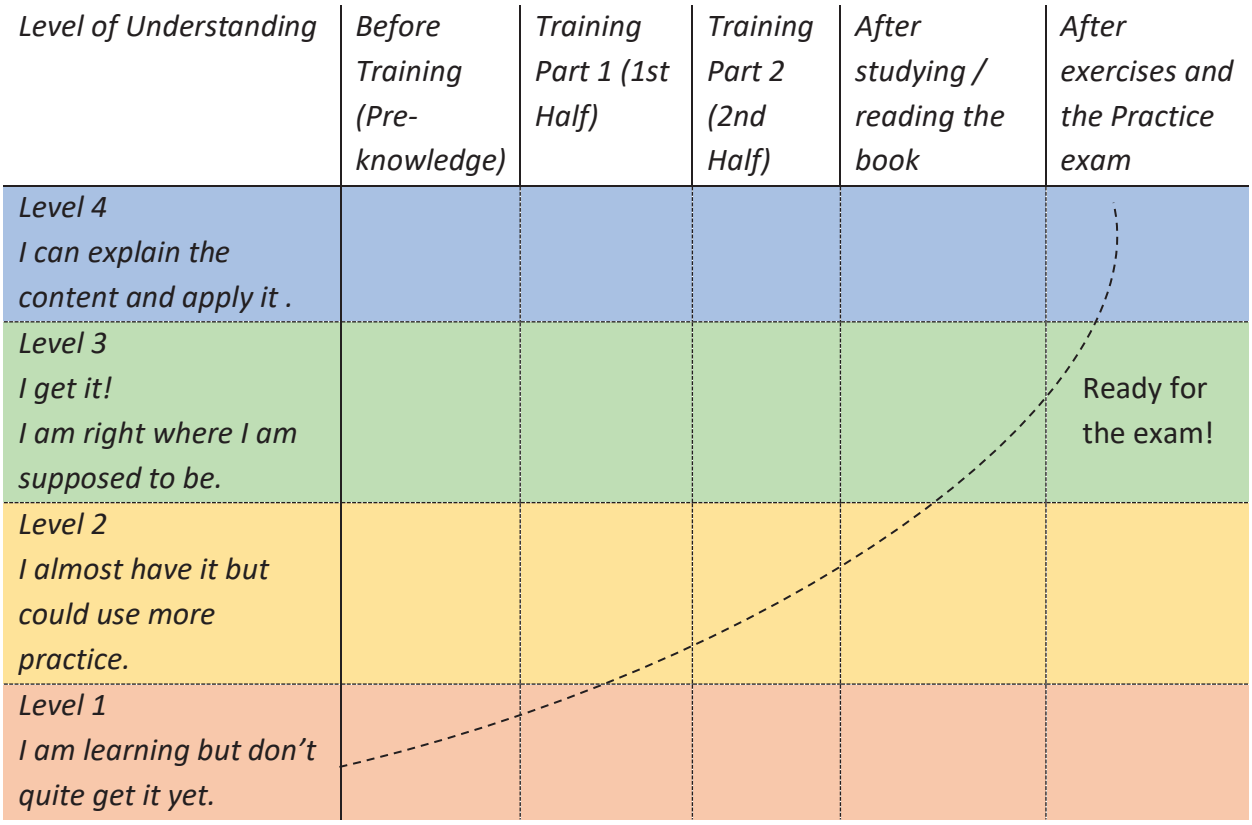
White paper Privacy and Data Protection Foundation 101

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.



(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 – 14:00	Module 2: Organizing data protection
14:00 – 15:00	Module 3: Practice of data protection
15:00 – 15:30	Practice questions & Evaluate
15:30 – 16:30	Sample Exam questions and review

Introduction

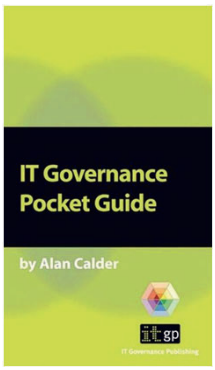
- Let's meet & Goals
- Terms
- Program

ABOUT THIS COURSE

Agenda
Privacy and Data Protection Essentials

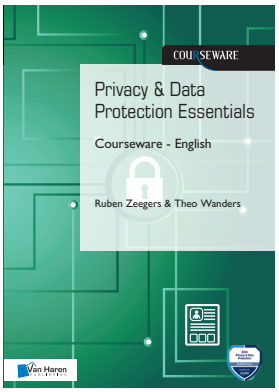
09:00 – 09:30	Introduction, About this course
09:30 – 12:00	Module 1: Privacy & data protection fundamentals & regulation
12:00 – 12:30	Lunch
12:30 – 14:00	Module 2: Organizing data protection
14:00 – 15:00	Module 3: Practice of data protection
15:00 – 15:30	Practice questions & Evaluate
15:30 – 16:30	Sample Exam questions and review

Literature



Study book

Whitepaper



Courseware

Trainer slides
(Included in Courseware)

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 Essentials (PDPE) 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

- 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.

Exam requirements

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 Personal data transfer to third countries[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%

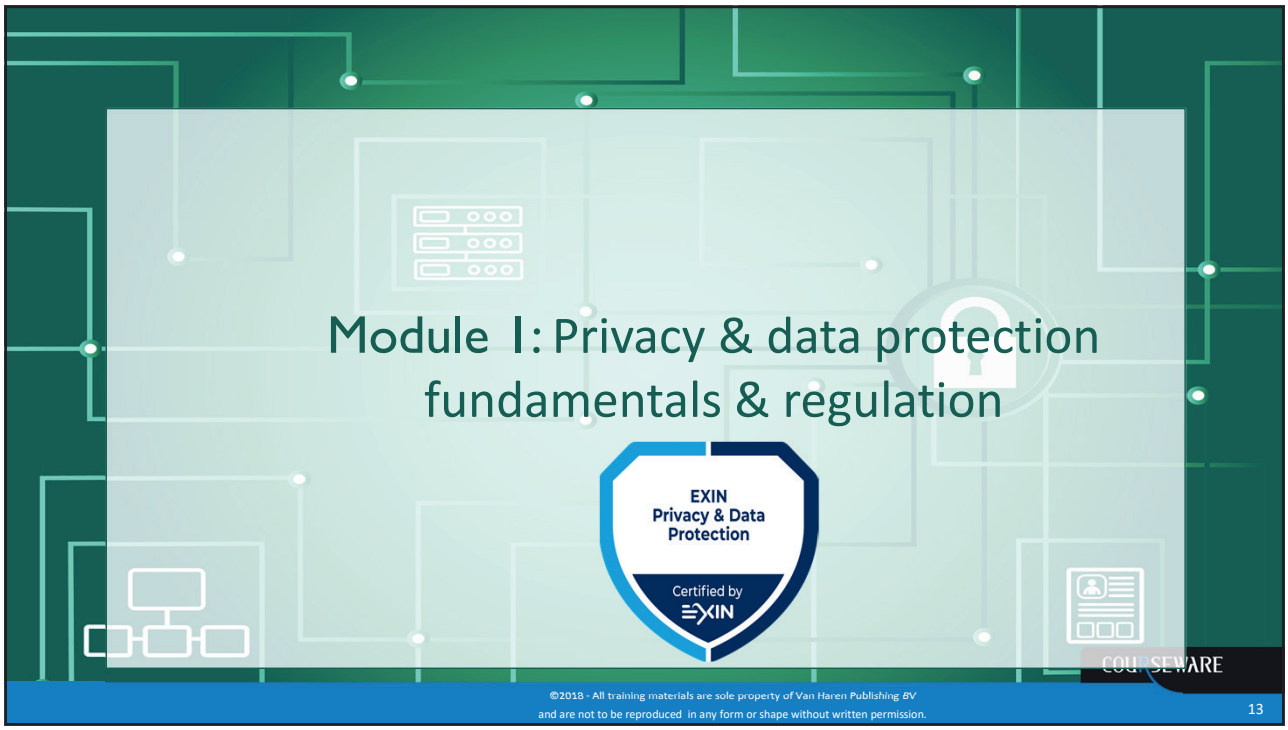
[1] Before the GDPR was introduced the *data protection authority* was the national authority in charge with the enforcement of regulation on data protection. In the GDPR it is now called the *supervisory authority.*

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

Exam specifications

- Examination type: Computer-based or paper-based multiple-choice questions
- Number of questions: 20
- Pass mark: 65%
- Open book/notes: No
- Electronic equipment/aides permitted: No
- Time allotted for examination: 30 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



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 tor the protection of the rights and freedoms of ethers.

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."

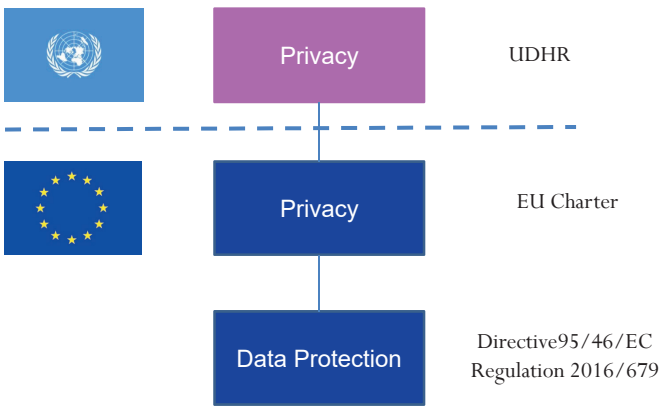
- Charter of Fundamental Rights of the European Union (2000)

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 apllied*

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)