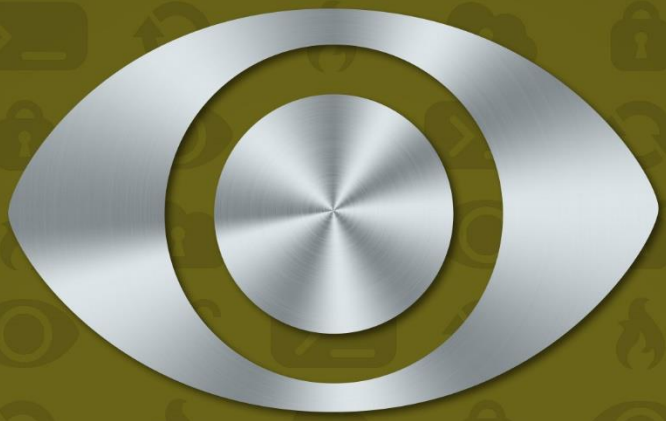

PRIVACY & DATA PROTECTION

PRACTITIONER

Exam Syllabus

SECO INSTITUTE

Table of contents

Disclaimer

The SECO-Institute has made every effort to ensure that the information included in this exam syllabus were correct at the time of publication. The SECO-institute does not assume and hereby disclaims any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Copyright notice

Copyright © SECO-Institute, 2018. All rights reserved

Context

This course constitutes the second level of the Certified Data Protection Officer certification track within the SECO-Institute's Cyber Security & Governance Certification Program. Successful completion of the Privacy & Data Protection Practitioner course provides candidates with sufficient knowledge to be able to continue with the Expert level and advance their career path to become a Certified Data Protection Officer. The Expert level of this certification track is currently under development.

Target audience

The Privacy & Data Protection Practitioner certificate is ideal for professionals who are, or expect to become, responsible for processes that involve or affect personal data. This includes, in particular:

- Data Protection Officers
- Privacy Officers
- Security specialists
- Managers who need to understand how the GDPR affects their activities
- Managers who need to incorporate data protection into their processes
- Project managers who need to embed data protection into their projects
- And finally, all those who are interested in the practical application of the GDPR

Exam information

The SECO-Institute offers its official Privacy & Data Protection Foundation courseware through accredited training centres where candidates are trained by accredited instructors. Candidates can take their exams at an accredited exam centre or book an exam directly with the SECO-Institute.

Attending a course is not a prerequisite for taking the exam.

Examination details

- Computer-based
- Multiple choice questions and essay-type questions
    - 10 multiple choice questions: 3 points per question
    - 5 short open-ended questions: 8 points per question
    - 1 essay question based on a case study: 30 points
- Time allotted: 120 minutes
- Pass mark: 60% (60 points out of 100 points)
- Open book/notes: not permitted
- Electronic equipment: not permitted

Rules to be observed by candidates: the SECO-Institute's Examination Rules and Regulations (https://www.seco-institute.org/html/filesystem/storeFolder/10/General-Terms-and-Conditions-for-participation-in-SECO-Institute-exams-2017-11.pdf)

Exam requirements

The following tables list the exam requirements and exam specifications.

Privacy & Data Protection Practitioner										
Requirements	1. Data Protection: Strategic Considerations 2. Data Protection Impact and Risk Assessment 3. Data Protection: Operations 4. Data Protection: Design and Implementation 5. Data Protection: Governance									
Required prior Knowledge/experience	Basic knowledge of privacy and data protection legislation, in particular of the EU's General Data Protection Regulation (GDPR), is required. Candidates who have limited knowledge of the GDPR should consider completing the Data Protection Foundation course before registering for the Practitioner level.									
Learning levels	Know	x	Understand	x	Apply	x	Analyse, Synthesise		Create	

Exam specifications

Bloom level
2. Understand
3. Apply

Requirements, specifications, testing levels				Bloom level
1.	**Data Protection: Strategic Considerations**			
	1.1	The candidate can draft a vision on data protection		2
		The candidate is able to:		
		1.1.1	Explain the importance of drawing up a vision statement	2
		1.1.2	List the content elements of a vision on data protection	2
Exam topics and terms			Corporate vision; vision on data protection; corporate ambitions, key success factors.	
	1.2	The candidate can describe the general principles that govern the processing of personal data. The candidate can explain why identifying such general principles is important.		2
		The candidate is able to:		
		1.2.1	List the most well-known data protection frameworks	2
		1.2.2	Describe the general principles on which the frameworks are based	2
		1.2.3	Explain what the general principles mean and why they are important	2
Exam topics and terms			GDPR provisions; data protection frameworks; lawfulness, fairness and transparency; purpose legitimacy and specification; data minimisation; accuracy and data quality; use, retention and disclosure limitation; information security (Confidentiality, Integrity and Availability); accountability; data transfer & adequacy; data subject rights; openness and notice.	
	1.3	The candidate can draft a strategic data protection policy and a privacy statement		3
		The candidate is able to:		
		1.3.1	Explain why it is necessary to have a data protection policy	2
		1.3.2	Describe the factors that should be taken into account when developing a policy	2
		1.3.3	Describe the structure, the content elements, and the characteristics of a good data protection policy	2
		1.3.4	Describe the factors that play a part in policy implementation	2
		1.3.5	Draft a data protection policy and draw up a GDPR-compliant privacy statement/privacy notice	3
Exam topics and terms			Data protection policy; privacy statement and privacy notice; policy assurance and policy maintenance; compliance management; GDPR requirements.	
	1.4	The candidate knows how to create data inventories		2
		The candidate is able to:		

		1.4.1	List different data mapping methods, create a data map, and explain how data protection requirements relate to the various phases of the data lifecycle	2
Exam topics and terms			Data inventory; data flow maps; information lifecycle; compliance.	

Requirements, specifications, testing levels				Bloom level
2.	**Data Protection Impact Assessment (DPIA) and Risk Management**			
	2.1	The candidate can carry out a basic data protection impact assessment		3
		The candidate is able to:		
		2.1.1	Define risk management and risk assessment/analysis	2
		2.1.2	Explain how a risk assessment matrix can be built	2
		2.1.3	Describe the factors that should be considered when selecting appropriate risk controls	2
		2.1.4	Describe the relationship between a data protection impact assessment and a data protection risk assessment	2
		2.1.5	Carry out a Data Protection Impact Assessment (DPIA)	3
Exam topics and terms			Risk, risk management and risk assessment; likelihood and impact; confidentiality, integrity and availability; risk assessment matrix; risk capacity, risk appetite and risk tolerance; risk assessment factors; threat actors; risk controls; risk-based approach.	
	2.2	The candidate knows how to create a GDPR-compliant DPIA model		3
		The candidate is able to:		
		2.2.1	Describe the GDPR's requirements for a DPIA	2
		2.2.2	Describe methods that can be used to perform a DPIA	2
		2.2.3	Sketch a DPIA model for a specific organisational context	3
Exam topics and terms			Data Protection Impact Assessment (DPIA); DPIA process; relevant 'Article 29 Data Protection Working Party' (European Data Protection Board) documentation.	
	2.3	The candidate knows what data protection requirements an organisation must meet under the GDPR		2
		The candidate is able to:		
		2.3.1	Describe data protection requirements in the context of implementing new practices, processes and procedures, and adapting existing practices, processes and procedures	2
		2.3.2	Describe data protection roles and responsibilities	2
		2.3.3	Describe data protection requirements in the context of technology	2
		2.3.4	Describe data protection requirements for projects	2
Exam topics and terms			Requirements relating to the business, information management, project management, information security management and operations. DPO; Data Protection Governance Board; process owner, data owner, data custodian and data user; technical measures; pseudonymisation; data protection by design and by default.	
	2.4	The candidate knows what data protection requirements apply to specific types of processing		2
		The candidate is able to:		
		2.4.1	Describe GDPR provisions relating to international data transfers	2
		2.4.2	Describe other legal requirements relating to data transfers	2

Exam topics and terms	Third countries and international organisations; adequacy decision; binding corporate rules; Privacy Shield.	

Requirements, specifications, testing levels				Bloom level
3.	**Data Protection and Operations**			
	3.1	The candidate knows how to organise data subject rights management		3
		The candidate is able to:		
		3.1.1	Describe what should be included in a data subject rights policy	2
		3.1.2	Describe the stages of the data lifecycle and match each stage with the relevant data subject rights	3
		3.1.3	Contribute to developing a process/system for handling data subject requests and draft a procedure for handling data subject complaints	
Exam topics and terms			Data lifecycle; data subject rights; request handling; complaints management; DPO.	
	3.2	The candidate knows how to manage data processing agreements in the contract management lifecycle		2
		The candidate is able to:		
		3.2.1	List roles and responsibilities involved in contract management	2
		3.2.2	Describe what must be included in a GDPR-compliant data processing agreement	2
		3.2.3	Describe appropriate technical and organisational security measures in the context of a data processing agreement	2
		3.2.4	Describe the controller's and processor's role in contract management	2
Exam topics and terms			Contract management lifecycle; data processing agreement; roles and responsibilities; technical and organisational security measures; controller and processor; accountability and liability	
	3.3	The candidate knows how to handle data breaches		3
		The candidate is able to:		
		3.3.1	Describe what a data breach is and what the main causes of a data breach are	3
		3.3.2	Describe potential risks posed by a data breach	2
		3.3.3	Describe how to prepare for a data breach	2
		3.3.4	Describe the content elements of a data breach response policy and the GDPR's data breach notification requirements	2
		3.3.5	Describe how to respond to a data breach and contain a data breach	3
		3.3.6	Draft a data breach procedure	
Exam topics and terms			Data breach procedure; data breach notification; data sensitivity.	
	3.4	The candidate knows how a data protection administration and documentation system can be constructed and maintained		3
		The candidate is able to:		
		3.4.1	Describe what documentation the controller and processor must create and maintain under the GDPR, and how the relevant documentation should be created and maintained	2
		3.4.2	Build a register of processing activities	3

Exam topics and terms			Data protection administration and documentation; role of the DPO; continuous change and improvement; register of processing activities; decision-making.	
	3.5		The candidate knows what activities are included in logging, monitoring and reporting	2
			The candidate is able to:	
		3.5.1	Define logging, monitoring and reporting	2
		3.5.2	Describe all aspects of the monitoring process	2
Exam topics and terms			Logging; registration; monitoring; alarm; reporting; follow-up; regulatory and legislative changes; compliance; risk; environment; types of monitoring.	

Requirements, specifications, testing levels				**Bloom level**
4.	**Data Protection: Design and Implementation**			
	4.1	The candidate can instil and enhance data protection awareness in an organisation		3
		The candidate is able to:		
		4.1.1	Summarise Bateson's theory on the determinants of human behaviour	2
		4.1.2	Summarise Ajzen's theory of planned behaviour	2
		4.1.3	Use behavioural theory basics to identify target groups for an awareness campaign	3
		4.1.4	Translate data protection risks into behavioural goals	2
		4.1.5	Explain the 5S (five-sphere) model for organisational change management	2
		4.1.6	Draft an awareness program action plan	3
Exam topics and terms			Awareness; behavioural change; Bateson's model; Ajzen's theory of planned behaviour.	
	4.2	The candidate can explain how to implement the principles of data protection by design and by default		2
		The candidate is able to:		
		4.2.1	Describe the principles of data protection by design and by default	2
		4.2.2	Describe privacy by design methodologies	2
		4.2.3	Explain how data protection can be embedded in the software development lifecycle	2
Exam topics and terms		Data protection by design and by default; the seven foundational principles; security by design; privacy by policy; privacy by architecture. Technical controls: data minimisation; obfuscation/data masking; access management; encryption. Data loss prevention; database logging. Least privilege; need to know; least trust; mandatory access control; segregation of duties; positive-sum vs zero-sum; end-to-end security; full lifecycle protection; visibility and transparency; database security; identity and access management.		
	4.3	The candidate knows how privacy-enhancing technologies can contribute to GDPR-compliance		2
		The candidate is able to:		
		4.3.1	Describe the most well-known privacy-enhancing technologies	2
		4.3.2	Explain how a layered security model works	2

Exam topics and terms	Privacy-enhancing technology (PET); anonymisation and pseudonymisation; cryptography and key management; metadata; layered security model; access control.	

Requirements, specifications, testing levels				Bloom level
5.	**Data Protection: Governance**			
	5.1	The candidate can explain how to design effective data protection reports		2
		The candidate is able to:		
		5.1.1	Describe what factors should be taken into account when designing data protection reports and what information the reports should contain	2
		5.1.2	Summarise how to develop a data protection metrics program	2
		5.1.3	Explain the concept of strategic monitoring	2
	5.2	The candidate can explain how the concepts of quality management systems can be applied to a data protection management system (DPMS)		2
		The candidate is able to:		
		5.2.1	Explain why implementing a data protection management system is essential for good data protection governance	2
		5.2.2	Describe how data protection governance should be effectuated	2
		5.2.3	List the DPO's tasks in developing and implementing a data protection management system	2
		5.2.4	Describe the building blocks of a data protection management system	2
Exam topics and terms			DPMS; governance.	
	5.3	The candidate can assist their organisation in demonstrating data protection compliance through data protection audits and third-party assurance		2
		The candidate is able to:		
		5.3.1	Describe the various areas of data protection compliance	2
		5.3.2	Describe the steps of a data protection audit process	2
		5.3.3	Describe what follow-up actions may be needed after receiving a data protection audit report	2
		5.3.4	List the powers of the supervisory authority and summarise the consequences of non-compliance	2
		5.3.5	Explain basic concepts relating to a third-party assurance process	2
Exam topics and terms			Governance; risk management; compliance audit; third party assurance.	

Literature

A	**SECO-Institute S-DPP course material**
Optional/ additional	
B	**General Data Protection Regulation (GDPR)** http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

Exam-literature matrix

Exam requirement	Exam specification	Literature (A, B)	Reference(s) Literature: A
1	1.1	A	Module 1, Section: Vision on Data Protection
	1.2	A	Module 1, Sections: • Data Protection Frameworks • Data Protection Principles
	1.3	A	Module 1, Sections: • Data Protection Policy • Privacy Notice
	1.4	A	Module 1, Section: Data Inventory
2	2.1	A	Module 2, Sections: • Risk Management • DPIA in the Context of the GDPR
	2.2	A	Module 2, Sections: • Risk Management (last slides) • DPIA in the Context of the GDPR

Exam requirement	Exam specification	Literature (A, B)	Reference(s) Literature: A

	2.3	A	Module 2, Section:
			• Data Protection Requirements
			  ○ Business
			  ○ Organisation
			  ○ Technical
			Module 4, Section:
			• Data Protection Requirements
			  ○ Projects

	2.4	A	Module 2, Section: Data Protection Requirements
3	3.1	A	Module 3, Sections: • Data Subject Rights Management • Complaints Procedure
	3.2	A	Module 3, Section: Contract management: Data Processing Agreements
	3.3	A	Module 3, Section: Data Breach Procedure
	3.4	A	Module 3, Section: Administration & Documentation
	3.5	A	Module 3, Section: Logging & Monitoring
4	4.1	A	Module 4, Section: Data Protection Awareness
	4.2	A	Module 4, Section: Privacy by Design/Default
	4.3	A	Module 4, Section: Privacy-Enhancing Technologies
5	5.1	A	Module 5, Sections: Data Protection Reports
	5.2	A	Module 5, Section: Data Protection Management System

Exam requirement	Exam specification	Literature (A, B)	Reference(s) Literature: A

	5.3	A	Module 5, Sections:
			
			• Compliance
			• Data Protection Audits
			  ○ Follow-up on Audit Outcomes
			  ○ Supervisory Authority
			  ○ Third Party Assurance

How to book your exam

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://go.proctoru.com/

Make sure you are well-prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book and take your exam at your convenience. It is up to you to decide where and when you will be tested.

System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. After you have completed the exam, the recordings will be checked by multiple proctors to see whether you comply with all the requirements.

Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after completing the test. The email will contain information on how to claim your certificate and digital badge, and how to use your title.

Certification Title

Upon successful completion of an exam, you can request your certification title from the SECO-Institute. To maintain a Practitioner certification, you need to earn and submit 20 Continuing Professional Education (CPE) credits yearly, a total of 60 credits over the three-year certification cycle. CPE requirements can be fulfilled by attending conferences, seminars, webinars or other trainings, through self-study, and through teaching activities and publications.

Digital badges

SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certifications. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges enable certification holders to convey to employers, potential employers and other interested parties the skills they have acquired to earn and maintain a specialised certification.

Claim your title at: https://www.seco-institute.org/claim-your-title

© SECO Institute 2019

All rights reserved. No part of this document or its contents may be adapted, translated, stored, reproduced and/or made public in any form or by any means, either electronically through print, (photo)copy, recording, in digital form or in any other way, without the prior written permission of the SECO Institute. Making this document public also explicitly includes its use within courses, lessons, trainings, seminars and other forms of instruction or demonstration.

This document is granted to those who are participating or have participated in a training, course, seminar, or similar event developed or authorised by the SECO Institute. The contents of this document, or parts thereof, may not be submitted or made available to third parties under whatever title without the prior explicit permission of the SECO Institute.

Although the SECO Institute has done everything to prevent irregularities in this document, errors may still occur. Therefore, any person who acts on the basis of the content of this document does so at his/her own risk and is aware of the fact that the SECO Institute cannot be held accountable for any possible damage ensuing from his/her actions.

The authors of this document have done their utmost to identify all possible rightful parties other than the SECO Institute. Should you be a rightful party, or represent one, or know one, and be of the opinion that this document unjustly contains copyrighted material, please do not hesitate to contact the SECO Institute.