PECB

When Recognition Matters

EXAM PREPARATION GUIDE

PECB Certified Data Protection Officer

The objective of the "PECB Certified Data Protection Officer" examination is to ensure that the candidate has acquired the knowledge and skills necessary to support an organization in effectively implementing and managing a compliance framework with regard to the protection of personal data based on GDPR.

The target population for this examination is:

- Project managers or consultants wanting to prepare and support an organization in the implementation of the new procedures and adoption of the new requisites presented in the GDPR, which will come into force by the 25th May, 2018;
- DPO and Senior Managers responsible for the personal data protection of an enterprise and the management of its risks;
- Members of an information security, incident management and business continuity team;
- Expert advisors in security of personal data;
- Technical and compliance experts preparing for a Data Protection Officer job

The exam content covers the following domains:

- **Domain 1:** Data Protection Concepts and Rights of the Data Subject
- **Domain 2:** Data Controllers, Processors and the DPO
- **Domain 3:** Planning the GDPR Compliance Project
- **Domain 4:** Data Protection Impact Assessment and Privacy Impact Assessment
- **Domain 5:** Data Protection Measures and Approaches
- **Domain 6:** Performance Evaluation, Monitoring and Measurement of the GDPR Compliance Project

The content of the exam is divided as the following:

Domain 1: Data Protection Concepts and Rights of the Data Subject

Main objective: To ensure that the Certified Data Protection Officer candidate can understand and interpret the GDPR objectives, scope, definitions, concepts, data protection principles and the rights of the data subjects

Competencies	Knowledge statements
1. Ability to understand the history of data protection regulations 2. Ability to understand legislations in different countries 3. Understand the role and general interest of the European Commission 4. Ability to understand the importance of the European data protection board, its members and tasks 5. Ability to explain the material and territorial scope of the GDPR, and where does it apply 6. Understand the important concepts and definitions of data protection necessary to comply with the regulation 7. Ability to understand the data protection principles required by GDPR 8. Ability to implement the necessary measures that ensure compliance to the basic principles of processing personal data, including accountability, transparency, lawfulness, purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality 9. Ability to understand the key concepts of GDPR 10. Ability to understand the right of the data subject 11. Ability to understand what measures are necessary to ensure compliance and protect the right of the data subjects	1. Knowledge of main data protection regulations and their history 2. Knowledge of the European Union responsibilities, interests and legislations. 3. Knowledge on the establishment of the European data protection board and its members tasks, including the tasks of the board chair 4. Knowledge of the importance of the fundamental right with regard to the protection of natural persons in relation to the processing of personal data 5. Knowledge of the different factors, such as economic and social integration, that affect the cooperation between the Member States in terms of exchanging personal data 6. Knowledge of the main definitions of GDPR that provide valuable information for an effective understanding and implementation of a compliance framework based on GDPR 7. Knowledge of the main data protection principles that provide valuable information for an effective understanding and implementation of a compliance framework based on GDPR 8. Knowledge of the appropriate measures for ensuring compliance with the basic principles of processing personal data 9. Knowledge on the key concepts provided by GDPR, including processors, controllers, DPO, restriction of processing, personal data, genetic data, etc. 10. Knowledge of data subject rights and access to personal data 11. Knowledge on how to determine the adequate measures for ensuring respect and protection of data subject's rights.

Domain 2: Data Controllers, Processors and the DPO

Main objective: To ensure that the Certified Data Protection Officer candidate can understand and determine the main tasks and responsibilities of the controller, the processor and the data protection officer and the importance of processing activities

Competencies	Knowledge statements
1. Ability to understand the importance of the controller and the processor 2. Ability to determine the roles and responsibilities of the controller and the processor 3. Ability to understand processing under the authority of the controller or processor 4. Understand the designation of the data protection officer 5. Understand the tasks and responsibilities of the data protection officer 6. Ability to understand the main activities of the DPO 7. Ability to understand the role of the DPO in relation to the DPIA and processing activities	1. Knowledge of the GDPR requirements that provide information regarding the controller and the processor 2. Knowledge of the appropriate technical and organizational measures that shall be implemented by the controller and the processor 3. Knowledge on who shall and who shall not process personal data as required by the GDPR 4. Knowledge of the necessary records of processing activities 5. Knowledge of the required process to designate a data protection officer 6. Knowledge of the professional qualities of the designated data protection officer 7. Knowledge on the GDPR requirements regarding the tasks of the DPO 8. Knowledge of the impacts that influence the performance of the DPO, including the controllers and the processors support 9. Knowledge on the professional qualifications required for the appointment of a DPO 10. Knowledge on how to allocate the necessary resources 11. Knowledge on the importance of processing personal data

Domain 3: Planning the GDPR Compliance Project

Main objective: To ensure that the Certified Data Protection Officer candidate can plan the implementation of the GDPR compliance project

Competencies	Knowledge statements
1. Ability to understand the business implications 2. Ability to conduct a gap analysis 3. Ability to assess security risks 4. Ability to explain the main issues and challenges in complying with the GDPR 5. Ability to prepare for the GDPR implementation 6. Ability to create and present a business case 7. Ability to establish the GDPR compliance project team 8. Ability to determine the required resources for the GDPR compliance project implementation 9. Ability to draft a project plan 10. Ability to fill and review a project plan 11. Ability to approve the project 12. Ability to create policy models 13. Ability to draft a data protection policy 14. Ability to publish a data protection policy 15. Ability to define an organizational structure for managing data protection	1. Knowledge of the GDPR business implications 2. Knowledge on how to conduct a gap analysis and determine what an organization wants to achieve by implementing the GDPR 3. Knowledge on the risk assessment process and risk prioritization 4. Knowledge on the main challenges that organizations can face during the implementation of the GDPR, including compliance with basic principles, rights of data subjects, notification of data breaches and issues that might appear such as administrative fines 5. Knowledge on how to raise awareness in terms of the personal data protection importance, on documenting information, acknowledging rights relevant to data subjects, data breaches, children's data and other GDPR requirements 6. Knowledge of the importance of the business case and its content 7. Knowledge of the roles and responsibilities of the project champion, project manager, project management team and interested parties 8. Knowledge of the types of resources needed to effectively implement the GDPR compliance project 9. Knowledge on the importance of the project plan and the reasons of using the project plan 10. Knowledge of the main elements of the project plan including the project charter, work break down structure, estimated cost, project deliverables, etc. 11. Knowledge on how to review the project objectives and success factors, the proposed method, deliverables, roles and responsibilities, and project documents 12. Knowledge of the key benefits of management commitment and the expected benefits of GDPR compliance project implementation 13. Knowledge of the general process of drafting a policy 14. Knowledge of the data protection policy objectives 15. Knowledge on how to publish the data protection policy 16. Knowledge on how to communicate the approved data protection policy and assess whether its objectives are being met

	17. Knowledge on how to develop a governance structure for data protection that fully meets requirements such as strong support from senior management

Domain 4: Data Protection Impact Assessment and Privacy Impact Assessment

Main objective: To ensure that the Certified Data Protection Officer candidate can understand the process of data mapping, data protection impact assessment and privacy impact assessment

Competencies	Knowledge statements
1. Ability to understand the process of data mapping 2. Understand the importance of recording the processing activities 3. Ability to understand the importance of the data mapping process 4. Ability to understand the data mapping recommended practices 5. Ability to understand the data mapping flows and data flow diagram 6. Ability to understand what does the data protection impact assessment addresses 7. Ability to understand the iterative process for carrying out a DPIA 8. Ability to determine when is it necessary to carry out a DPIA 9. Ability to conduct a data protection impact assessment 10. Ability to understand the benefits of privacy impact assessment 11. Ability to understand how to conduct privacy impact assessment	1. Knowledge on how to create data mappings between different data models, and to determine what types of personal data does an organization processes 2. Knowledge on how to develop and maintain the records of processing activities 3. Knowledge of the data mapping process steps 4. Knowledge on what categories of data are being stored, who owns and has access to the data that is being stored, and to which recipients the data is disclosed 5. Knowledge of the data mapping recommended practices such as construction and maintenance 6. Knowledge of the key elements of the data mapping flows and creation of a data flow diagram 7. Knowledge of the DPIA importance and of the processing operations that it addresses 8. Knowledge of the iterative process steps for carrying out a DPIA including steps such as foreseen processing, assessment of necessity, foreseen measures to demonstrate compliance, risk assessment, foreseen measures to address the risk, documentation, monitoring and review 9. Knowledge of the criteria that shall be considered when the processing of personal data is likely to result in a high risk 10. Knowledge of the measures that shall be implemented if the data protection impact assessment indicates that processing will result in a high risk 11. Knowledge of the PIA benefits, including, identification of privacy impacts, reviewing a new information system, providing input for privacy protection design, sharing and mitigating privacy

	risks with stakeholders, etc. 12. Knowledge of the WP29 and ISO/IEC 29134 guidelines on how to conduct a PIA

Domain 5: Data Protection Measures and Approaches

Main objective: To ensure that the Certified Data Protection Officer candidate can determine the necessary measures that shall be implemented to ensure safe processing of personal data and compliance with GDPR and interpret the relationship between GDPR, Information Security, Business Continuity and Incident Management

Competencies	Knowledge statements
1. Ability to understand the relationship between GDPR and Information Security 2. Ability to define the steps to cybersecurity 3. Ability to determine the necessary technical and organizational measures to ensure the security of processing 4. Ability to ensure the security of personal data including its processing 5. Ability to determine the necessary technical and organizational measures to ensure the security of processing 6. Ability to understand the relationship between GDPR and Business Continuity 7. Ability to define what steps help organizations ensure compliance with GDPR 8. Ability to understand the relationship between GDPR and Incident Management 9. Ability to understand the importance of notifying any personal data breach without undue delay 10. Ability to communicate the personal data breach to the data subject 11. Ability to prepare an incident response plan	1. Knowledge on what aspects of Information Security can compliance with the GDPR help 2. Knowledge of data centric cybersecurity strategy benefits including improvement of data security awareness within an organization, identification of the most crucial data, reduced costs, increase in the effectiveness of the DLP solutions, ensure security policy consistency and safety encouragement 3. Knowledge on the 10 steps to cybersecurity, namely the information risk management regime, security configuration, network security, managing user privileges, user education, incident management, malware protection, monitoring, removable media control, home and mobile working 4. Knowledge on the information security strategies steps and the main security related aspects such as people, processes and technology 5. Knowledge of the appropriate technical and organizational measures such as encryption of data and pseudonymisation 6. Knowledge on how to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services 7. Knowledge on how to restore the availability and access of personal data in a timely manner in the event of a physical or technical incident 8. Knowledge on what parts of the Business Continuity can compliance with the GDPR help 9. Knowledge on how to establish new data policies, reduce of the impact of the known risks, encourage education and training, set customer consent rules and create a data policy for outdated data 10. Knowledge on what aspects of the Incident

	Management can compliance with the GDPR help 11. Knowledge of the required time for notifying supervisory authorities regarding the personal data breach 12. Knowledge on the appropriate communication methods as means for notifying the data subject regarding the personal data breach 13. Knowledge on how to establish an incident response plan based on the incident management process

Domain 6: Performance Evaluation, Monitoring and Measurement of the GDPR Compliance Project

Main objective: To ensure that the Certified Data Protection Officer candidate can evaluate, monitor and measure the performance of the GDPR compliance project

Competencies	Knowledge statements
1. Ability to understand and determine measurement objectives 2. Ability to conduct evaluations of the GDPR compliance project to ensure continual ongoing stability, adequacy and effectiveness 3. Ability to determine which activities, processes and systems should be monitored 4. Ability to report the measurement results of the GDPR compliance project performance 5. Ability to conduct internal audits 6. Ability to designate a responsible person to conduct internal audit 7. Ability to perform audit activities 8. Ability to establish and review a GDPR audit checklist 9. Ability to understand the advantages and disadvantages of a continual internal audit programme 10. Ability to understand the principles and concepts related to continual improvement 11. Ability to continually improve the GDPR compliance project	1. Knowledge on what controls need to be measured and monitored 2. Knowledge on when to monitor, measure, analyze and evaluate performance of the GDPR compliance project 3. Knowledge on who will monitor, measure, analyze and evaluate the performance of the GDPR compliance project 4. Knowledge on how to monitor activities, processes and systems including incident management, physical and environmental security management, risk assessment process, security awareness and training, etc. 5. Knowledge on how to report the measurement results by using scorecards or strategic dashboards, tactical and operational dashboards, reports and gauges. 6. Knowledge of the role of the internal audit function related to the GDPR 7. Knowledge of the roles and responsibilities of the designated person to conduct an internal audit 8. Knowledge of the audit activities including collection of evidence from different sources of information, usage of appropriate audit procedures, gathering audit evidence, evaluation of audit evidence against the audit criteria, audit review and audit conclusion 9. Knowledge of the GDPR audit checklist elements including data governance and accountability,

	privacy notices, breach notification, data processors and international transfers, lawfulness of processing and consent, data subject rights, security and privacy by design and default 10. Knowledge of the main concepts related to continual improvement 11. Knowledge on how to continually monitor the change factors that influence GDPR compliance project effectiveness

Based on these six domains and their relevance, twelve (12) questions are included in the exam, as summarized in the following table:

			Level of understanding (Cognitive/Taxonomy) Required					
		Points per question	Questions that measure comprehension, application and analysis	Questions that measure Synthesis and Evaluation	Number of questions per competency domain	% of test devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency/Domains	Data protection principles and rights of the data subjects	10		X	2	16.66	15	20.01
		5	X					
	Data controllers, processors and the data protection officer	10	X		2	16.66	15	20.01
		5	X					
	Planning the GDPR compliance project	5	X		1	8.33	5	6.67
	Data protection impact assessment and privacy impact assessment	5		X	1	8.33	5	6.67
	Data protection measures and approaches	10		X	5	41.65	30	40.02
		5	X					
		5		X				
		5		X				
		5	X					
	Performance evaluation, monitoring and measurement of the GDPR compliance project	5	X		1	8.33	5	6.67
	Total Points	75						
	Number of questions per level of understanding		6	6				
	% of test devoted to each level of understanding (cognitive taxonomy)		50	50				

The passing score is established at 70%.

After successfully passing the exam, candidates will be able to apply for the credentials of PECB Certified Data Protection Officer, depending on their level of experience.

TAKE A CERTIFICATION EXAM

Candidates will be required to arrive at least thirty (30) minutes before the beginning of the certification exam. Candidates arriving late will not be given additional time to compensate for the delayed arrival, and may be denied entry to the examination room (if they arrive more than 5 minutes after the beginning of the exam scheduled time).

All candidates shall present a valid identity card with a picture such as a driver's license or a government ID to the invigilator.

The exam duration is three (3) hours. Non-native speakers receive an additional half an hour.

The exam contains essay type questions. This type of format was selected as a means of determining whether an examinee can clearly answer training related questions, by assessing problem solving techniques and formulating arguments supported with reasoning and evidence. The exam is set to be "open book", and does not measure the recall of data or information. The examination evaluates the candidates' comprehension, application and analyzing skills. Therefore, candidates will have to justify their answers by providing concrete explanations as to demonstrate that they have understood the training's concepts. At the end of this document, you will find samples of exam questions and potential answers.

As the exam is "open book", candidates are authorized to use:

- A copy of the General Data Protection Regulation;
- Course notes from the Participant Handout;
- Any personal notes made by the student during the course; and
- A hard copy dictionary.

All attempt to copy, collude or otherwise cheat during the exam will automatically lead to the exam's failure.

PECB exams are available in English. For availability of the exam in a language other than English, please contact examination@pecb.com

RECEIVE YOUR EXAM RESULTS

Results will be communicated by email within a period of 6 to 8 weeks from your examination date. The candidate will be provided with only two possible examination results: Pass or Fail.

Candidates who successfully complete the examination will be able to apply for a certified scheme.

In the case of a failure, the results will be accompanied by the list of domains in which the candidate had a low grade, to provide preparation guidance in case of retaking the exam.

Candidates who disagree with the exam results may file a complaint. For more information, please refer to www.pecb.com

EXAM RETAKE POLICY

There is no limit on the number of times a candidate may retake an exam. However, there are some limitations in terms of allowed time-frame in between exam retakes, such as:

- If a candidate does not pass the exam on the first attempt, he/she must wait 15 days for the next attempt (1st retake). Retake fee applies.

Note: *Students, who have completed the full training but failed the written exam, are eligible to retake the exam once for free within a 12 month period from the initial date of the exam*.

- If a candidate does not pass the exam on the second attempt, he/she must wait 3 months (from the initial date of the exam) for the next attempt (2nd retake). Retake fee applies.
- If a candidate does not pass the exam on the third attempt, he/she must wait 6 months (from the initial date of the exam) for the next attempt (3rd retake). Retake fee applies.

After the fourth attempt, a waiting period of 12 months from the last session date is required, in order for candidate to sit again for the same exam. Regular fee applies.

For the candidates that fail the exam in the 2nd retake, PECB recommends to attend an official training in order to be better prepared for the exam.

To arrange exam retakes (date, time, place, costs), the candidate needs to contact the PECB partner who has initially organized the session.

CLOSING FILES

Closing a file is equivalent to rejecting a candidate's application. As a result, when candidates request that their file be reopened, PECB will no longer be bound by the conditions, standards, policies, candidate handbook or exam preparation guide that were in effect before their file was closed.

Candidates who want to request that their file be reopened must do so in writing, and pay the required fees.

EXAMINATION SECURITY

A significant component of a successful and respected professional certification credential is maintaining the security and confidentiality of the examination. PECB relies upon the ethical behavior of certificate holders and applicants to maintain the security and confidentiality of PECB examinations. If someone holding PECB credentials reveals information about PECB examination content, he/she is considered to have violated the PECB Code of Ethics. PECB will take action against individuals who violate PECB Policies and the Code of Ethics. Actions taken may include permanently barring individuals from pursuing PECB credentials and revoking certifications from those who have been awarded the credential. PECB will also pursue legal remedies against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

SAMPLE EXAM QUESTIONS AND POSSIBLE ANSWERS

1. The purpose of the GDPR

GDPR considers the protection of natural persons in relation to the processing of personal data as a fundamental right. Please prepare a summary explaining the purpose of this regulation and the areas that the GDPR intends to contribute in.

Possible Answer:

Purposes of this regulation are to:

- *Establish standardized data protection laws over all European countries;*
- *Eliminate inconsistencies in national laws;*
- *Raise the bar to provide better privacy protection for individuals;*
- *Update the law to better address contemporary privacy challenges, such as those posed by the internet, social media, big data" and behavioral marketing;*
- *Reduce the costly administrative burdens for organizations dealing with multiple data protection authorities.*

This Regulation is intended to contribute to the security and justice area, as well as to the economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

2. Data protection officer

Please determine what tasks shall be assigned to the data protection officer, in order to assist the controllers and processors ensure compliance with the regulation.

Possible answer:

The data protection officer shall be involved properly and in a timely manner in all issues related to the protection of the personal data.

Some of the tasks of the data protection officer include:

Having an advisory role by:

- *Providing information and advices to the data controller, data processor and employees who carry out processing of their obligations in compliance with GDPR*
- *Provide advices regarding the data protection impact assessment (upon request)*

Monitoring:

- *Monitor compliance with GDPR*
- *Monitor compliance with internal policies*

- *Monitor compliance with other data protection legislations*
- *Monitor the performance of the DPIA (upon request)*

Other tasks

- *Cooperate with supervisory authority*
- *Act as a contact point for the supervisory authorities on issues relating to processing*

3. Data Protection Measures

Please define the measures that an organization can implement to demonstrate compliance with the following:

Possible Answer:

Transparency of data collection:

- *Establish policies;*
- *Set time limits;*
- *Conduct periodic review;*
- *Create supported operating systems;*
- *Turn on automated updates.*

Privacy and data breach*:*

- *Ensure that staff comprehends that data breach is more than the loss of personal data;*
- *Make sure that there is an internal breach reporting procedure in place;*
- *Make sure that investigation and internal reporting procedures are in place*.