PECB BEYOND RECOGNITION

Candidate Handbook

Certified Data Protection Officer

PECB

Table of Contents

SECTION I: INTRODUCTION

About PECB

PECB is a certification body which provides education[1] and certification in accordance with ISO/IEC 17024 for individuals on a wide range of disciplines.

We help professionals show commitment and competence by providing them with valuable evaluation and certification services against internationally recognized standards. Our mission is to provide services that inspire trust and continual improvement, demonstrate recognition, and benefit the society as a whole.

The key objectives of PECB are:

1. Establishing the minimum requirements necessary to certify professionals
2. Reviewing and verifying the qualifications of applicant to ensure they are eligible to apply for certification
3. Developing and maintaining reliable certification evaluations
4. Granting certifications to qualified candidates, maintaining records, and publishing a directory of the holders of a valid certification
5. Establishing requirements for the periodic renewal of certification and ensuring compliance with those requirements
6. Ensuring that candidates meet ethical standards in their professional practice
7. Representing its members, where appropriate, in matters of common interest
8. Promoting the benefits of certification to organizations, employers, public officials, practitioners in related fields, and the public

[1] Education refers to training courses developed by PECB, and offered globally through our network of partners.

The Value of PECB Certification

Why Choose PECB as Your Certification Body?

Global Recognition
Our certifications are internationally recognized and accredited by the International Accreditation Service (IAS); signatory of IAF Multilateral Recognition Arrangement (MLA) which ensures mutual recognition of accredited certification between signatories to the MLA and acceptance of accredited certification in many markets. Therefore, professionals who pursue a PECB certification credential will benefit from PECB's recognition in domestic and international markets.

Competent Personnel
The core team of PECB consists of competent individuals who have relevant sector-specific experience. All of our employees hold professional credentials and are constantly trained to provide more than satisfactory services to our clients.

Compliance with Standards
Our certifications are a demonstration of compliance with ISO/IEC 17024. They ensure that the standard requirements have been fulfilled and validated with the adequate consistency, professionalism, and impartiality.

Customer Service
We are a customer-centered company and treat all our customers with value, importance, professionalism, and honesty. PECB has a team of experts dedicated to support customer requests, problems, concerns, needs, and opinions. We do our best to maintain a 24-hours maximum response time without compromising the quality of the service.

PECB Code of Ethics

PECB professionals will:

1. Conduct themselves professionally, with honesty, accuracy, fairness, responsibility, and independence
2. Act at all times solely in the best interest of their employer, their clients, the public, and the profession, by adhering to the professional standards and applicable techniques while offering professional services
3. Maintain competency in their respective fields and strive to constantly improve their professional capabilities
4. Offer only professional services for which they are qualified to perform, and adequately inform clients about the nature of the proposed services, including any relevant concerns or risks
5. Inform each employer or client of any business interests or affiliations that might influence their judgment or impair their fairness
6. Treat in a confidential and private manner the information acquired during professional and business dealings of any present or former employer or client
7. Comply with all laws and regulations of the jurisdictions where professional activities are conducted
8. Respect the intellectual property and contributions of others
9. Not, intentionally or otherwise, communicate false or falsified information that may compromise the integrity of the evaluation process of a candidate for a professional designation
10. Not act in any manner that could compromise the reputation of PECB or its certification programs
11. Fully cooperate on the inquiry following a claimed infringement of this Code of Ethics

The full version of the PECB Code of Ethics can be downloaded here.

Introduction to Certified Data Protection Officer

European Union (EU) citizens have their personal data collected and processed by different organizations worldwide. As part of the efforts to standardize data protection laws for EU citizens, the EU created the General Data Protection Regulation (GDPR), which came into effect in 2018. It aims to ensure the protection of personal data and fundamental rights and the freedoms of natural persons of the EU, regardless of the location of the organizations that process their data.

Data protection officers (DPOs) are an essential component of any organization that wants to ensure GDPR compliance, especially if the organization find this process difficult. Moreover, in many situations, appointing a DPO is a mandatory requirement of the GDPR. This makes certified DPOs increasingly in-demand positions in today's market.

The "Certified Data Protection Officer" credential is a professional certification for individuals aiming to demonstrate the competence to assist an organization in ensuring compliance with the GDPR requirements.

It is important to understand that PECB certifications are not a license or a mere membership. They represent peer recognition that an individual has demonstrated proficiency in, and comprehension of, a set of competencies. PECB certifications are awarded to candidates that can demonstrate experience and have passed a standardized exam in the certification area.

This document specifies the PECB Certified Data Protection Officer certification scheme in compliance with ISO/IEC 17024:2012. This candidate handbook also contains information about the process by which candidates may earn and maintain their credentials. It is very important that you read all the information included in this candidate handbook before completing and submitting your application. If you have questions after reading it, please contact the PECB international office at certification@pecb.com

SECTION II: PECB CERTIFICATION PROCESS AND EXAMINATION PREPARATION, RULES, AND POLICIES

Decide Which Certification Is Right for You

All PECB certifications have specific education and professional experience requirements. To determine the right credential for you, verify the eligibility criteria for various certifications and your professional needs.

Prepare and Schedule the Exam

All candidates are responsible for their own study and preparation for certification exams. No specific set of training courses or curriculum of study is required as part of the certification process. Nevertheless, attending a training course can significantly increase candidates' chances of successfully passing a PECB exam.

To schedule an exam, candidates have two options:

1. Contact one of our partners who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Partners. The PECB training course schedule is also available on Training Events.
2. Take a PECB exam remotely from their home or any location they desire through the PECB Exam application, which can be accessed here: Exam Events.

To learn more about exams, competency domains, and knowledge statements, please refer to *Section III* of this document.

Application Fees for Examination and Certification

PECB offers direct exams, where a candidate can sit for the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000
- Manager Exam: $700
- Foundation and Transition Exam: $500

The application fee for certification is $500.

For all candidates that have followed the training course and taken the exam with one of PECB's partners, the application fee includes the costs associated with examination, application for certification, and the first year of Annual Maintenance Fee (AMF) only.

Competency Domains

The objective of the PECB Certified Data Protection Officer exam is to ensure that the candidate has acquired the necessary expertise to support an organization in implementing, managing, and maintaining a compliance framework for data protection based on the GDPR.

The Certified Data Protection Officer certification is intended for:

- Managers or consultants seeking to prepare and support an organization in planning, implementing, and maintaining a compliance program based on the GDPR
- DPOs and individuals responsible for maintaining conformity to the GDPR requirements
- Members of information security, incident management, and business continuity teams

- Technical and compliance experts seeking to prepare for a DPO role
- Expert advisors involved in the security of personal data

The content of the exam is divided as follows:

- **Domain 1:** Data protection concepts, general data protection regulation (GDPR), and compliance measures
- **Domain 2:** Roles and responsibilities of the data controllers, subcontractors, processors and the data protection officer (DPO)
- **Domain 3**: Technical and organizational measures for data protection

Domain 1: Data protection concepts, general data protection regulation (GDPR), and compliance measures **Main objective:** Ensure that the candidate understands and is able to interpret GDPR objectives, scope, definitions, concepts, principles, and the rights of the data subjects	
Competencies	**Knowledge statements**
1. Ability to understand the importance of the european data protection board (EDPB), its members and tasks 2. Ability to explain the material and territorial scope of the GDPR, and where it applies 3. Ability to understand the important concepts and definitions of data protection necessary to comply with the regulation 4. Ability to explain the main issues and challenges in complying with the GDPR 5. Ability to understand the data protection principles required by the GDPR 6. Ability to implement the necessary measures that ensure compliance with the basic principles of processing personal data, including accountability, transparency, lawfulness, purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality 7. Ability to identify the legal basis for the processing of data 8. Ability to understand the key concepts of GDPR 9. Ability to understand the rights of data subjects	1. Knowledge of the importance of the fundamental rights with regard to the protection of natural persons in relation to the processing of personal data 2. 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 3. Knowledge of GDPR business implications 4. Knowledge of the main definitions of GDPR that provide valuable information for an effective understanding and implementation of a compliance framework based on GDPR 5. Knowledge of the main data protection principles that provide valuable information for an effective understanding and implementation of a compliance framework based on GDPR 6. Knowledge of the appropriate measures for ensuring compliance with the basic principles of processing personal data 7. Knowledge of the key concepts provided by GDPR, including processors, controllers, DPOs, restriction of processing, personal data, genetic data, etc 8. Knowledge of data subject rights and access to personal data

10. Ability to understand what measures are necessary to ensure compliance with and protect the rights of data subjects 11. Ability to establish procedures designed to receive and manage applications for the exercise of the rights and freedoms of the data subject concerned 12. Ability to understand the requirements for the information to be provided to the data subject for the exercise of the rights of the data subject 13. Ability to determine and establish appropriate measures in order to provide transparent information to the data subject 14. Ability to prepare for GDPR implementation 15. Ability to create and present a business case 16. Ability to conduct a gap analysis 17. Ability to establish GDPR compliance project team 18. Ability to determine the required resources for the GDPR compliance project implementation 19. Ability to draft and review a project plan 20. Ability to understand the designation of the data protection officer 21. Ability to understand the tasks and responsibilities of the data protection officer 22. Ability to understand the main activities of the data protection officer 23. Ability to develop policy models 24. Ability to draft a data protection policy 25. Ability to publish a data protection policy 26. Ability to identify the existence of data transfers outside the EU/EEA to third countries or international organizations 27. Ability to conduct internal audits 28. Ability to designate a responsible person to conduct internal audits 29. Ability to perform audit activities 30. Ability to establish and review a GDPR audit checklist	9. Knowledge of the requirements for lawfulness of processing 10. Knowledge of the required information provided to the data subject when data are collected from the data subject 11. Knowledge of the requirement for the provision of information to the data subject in a concise, transparent, intelligible and easily accessible form, and the tools, methodologies and mechanisms to be used 12. Knowledge of conducting a gap analysis and determining what an organization aims to achieve by implementing GDPR 13. Knowledge of the importance of the business case and its content 14. Knowledge of the roles and responsibilities of the project champion, project manager, project management team and interested parties 15. Knowledge of the types of resources needed to effectively implement GDPR compliance project 16. Knowledge of the importance of the project plan and reasons for using it 17. Knowledge of the main elements of the project plan including the project charter, work breakdown structure, estimated costs, project deliverables, etc 18. Knowledge of how to review the project objectives and success factors, the proposed method, deliverables, roles and responsibilities, and project documents 19. Knowledge of the key benefits of management commitment and the expected benefits of GDPR compliance project implementation 20. Knowledge of the required processes to designate a data protection officer 21. Knowledge of the professional qualities of the designated data protection officer 22. Knowledge of GDPR requirements regarding the tasks of the data protection officer 23. Knowledge of the impacts that influence the performance of the data protection officer, including the controllers and the support of processors 24. Knowledge of the professional qualifications required for the appointment of a data protection officer

	25. Knowledge of how to allocate the necessary resources 26. Knowledge of how to establish new data policies, reduce the impact of the known risks, encourage education and training, set customer consent rules, and create a data policy for outdated data 27. Knowledge of the general process of drafting a policy 28. Knowledge of the data protection policy objectives 29. Knowledge of how to publish the data protection policy 30. Knowledge of how to communicate the approved data protection policy and assess if its objectives are met 31. Knowledge of the legal instruments that are provided by GDPR for transfers of data outside EU/EEA to third countries or international organizations (approved codes of conduct, approved certification mechanisms, transfers based on adequacy decisions, binding corporate rules, standard contractual clauses and derogations) 32. Knowledge of the role of the internal audit function related to GDPR 33. Knowledge of the roles and responsibilities of the designated person to conduct an internal audit 34. Knowledge of the audit activities including the 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 35. Knowledge of GDPR audit checklist elements, including data governance and accountability, privacy notices, breach notifications, data processors and international transfers, lawfulness of processing and consent, data subject rights, and security and privacy by design and default

PECB

Domain 2: Roles and responsibilities of the data controllers, subcontractors, processors and the data protection officer (DPO)

Main objective: Ensure that the candidate is able to determine the main tasks and responsibilities of the controller, processor, data protection officer, and the importance of processing activities, and ensure that the candidate understands the process of data mapping and data protection impact assessment (DPIA)

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. Ability to understand the role of DPO in relation to DPIA and processing activities 5. Ability to understand the process of data mapping 6. Ability to understand the importance of the data mapping process 7. Ability to understand the data mapping recommended practices 8. Ability to understand the data mapping flows and data flow diagrams 9. Ability to understand the importance of recording the processing activities 10. Ability to identify when the organization is required to maintain a record of processing activities under its responsibility 11. Ability to draft and maintain the records as set out in Article 30 of GDPR 12. Ability to establish and maintain a processing activity register 13. Ability to understand what is covered by the data protection impact assessment (DPIA) 14. Ability to understand the iterative process for carrying out a DPIA 15. Ability to determine when it is (or is not) necessary to perform a DPIA 16. Ability to conduct and provide advice on DPIA 17. Ability to assess security risks	1. Knowledge of GDPR requirements that provide information about 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 of who shall and who shall not process personal data as required by GDPR 4. Knowledge of the importance of processing personal data 5. Knowledge of how to create data mappings between different data models and to determine what types of personal data an organization processes 6. Knowledge of how to develop and maintain the records of processing activities necessary to maintain compliance with GDPR requirements 7. Knowledge of the steps of the data mapping process 8. Knowledge of what categories of data are being stored, who owns and has access to the data that are being stored, and to which recipients the data are disclosed 9. Knowledge of the data mapping recommended practices such as construction and maintenance 10. Knowledge of the key elements of the data mapping flows and creation of a data flow diagram 11. Knowledge of DPIA importance and of the processing operations that it addresses 12. Knowledge of the iterative process steps for performing a DPIA including steps such as foreseen processing, assessment of necessity, foreseen measures to demonstrate compliance,

18. Ability to identify personal data breaches that require notification to the competent supervisory authority 19. Ability to understand the importance of notifying any personal data breach without undue delay 20. Ability to identify personal data breaches that must be communicated to the data subjects 21. Ability to communicate the personal data breach to the data subject 22. Ability to identify data protection measures from the design stage and integrate the necessary safeguards into the processing 23. Ability to implement appropriate technical and organizational measures for ensuring that by default only personal data necessary for the processing activities are collected	risk assessment, foreseen measures to address the risk, documentation, monitoring and review 13. Knowledge of the criteria that shall be considered when the processing of personal data is likely to result in a high risk 14. Knowledge of the measures that shall be implemented if DPIA indicates that processing will result in a high risk 15. Knowledge of DPIA benefits, including identification of privacy impacts, reviewing of a new information system, providing input for privacy protection design, sharing and mitigating privacy risks with stakeholders, etc 16. Knowledge of WP29 and ISO/IEC 29134 guidelines on how to conduct a DPIA 17. Knowledge of the main challenges that organizations may face during the implementation of GDPR, including compliance with basic principles, rights of data subjects, notification of data breaches and issues that might appear 18. Knowledge of the time required for notifying supervisory authorities regarding the personal data breach 19. Knowledge of the appropriate communication methods as means of notifying the data subject regarding the personal data breach 20. Knowledge of how to raise awareness about the importance of personal data protection, documenting information, acknowledging the rights relevant to data subjects, data breaches, children's data and other GDPR requirements 21. Knowledge of the risk assessment process and risk prioritization 22. Knowledge of the appropriate technical and organizational measures used to ensure data protection by design, such as pseudonymization, encryption, anonymization, etc.

PECB

Domain 3: Technical and organizational measures for data protection

Main objective: Ensure that the candidate can determine the necessary measures that shall be implemented to ensure the safe processing of personal data and compliance with GDPR, interpret the relationship between GDPR, information security, business continuity and incident management, and make sure that the candidate can evaluate, monitor and measure the performance of GDPR compliance project

Competencies	Knowledge statements
1. Ability to define an organizational structure for managing data protection 2. Ability to understand the relationship between GDPR and information security 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 the steps that help organizations ensure compliance with GDPR 8. Ability to manage and maintain the relationship with the supervisory authority, including, among others, communication, consultation, responding to their requests, and acting upon their requests 9. Ability to understand the relationship between GDPR and incident management 10. Ability to prepare an incident response plan 11. Ability to develop, implement and conduct training and awareness programs regarding data protection for staff and senior management 12. Ability to understand and determine measurement objectives 13. Ability to determine what activities, processes and systems should be monitored 14. Ability to report the measurement results of GDPR compliance project performance	1. Knowledge of how to develop a governance structure for data protection that fully meets the requirements (eg, strong support from senior management) 2. Knowledge of information security aspects that an organization complies with by implementing GDPR 3. 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 DLP solutions, security policy consistency and safety encouragement 4. Knowledge of the ten (10) steps of cybersecurity, including 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 5. Knowledge of information security strategy steps and the main security related aspects (eg, people, processes and technology) 6. Knowledge of the appropriate technical and organizational measures such as data minimization, encryption, pseudonymization, and physical security 7. Knowledge of how to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services 8. Knowledge of how to restore the availability and access of personal data in a timely manner in case of a physical or technical incident

15. Ability to conduct evaluations of GDPR compliance project to ensure continual ongoing stability, adequacy and effectiveness 16. Ability to understand the principles and concepts related to continual improvement 17. Ability to continually improve GDPR compliance project	9. Knowledge of business continuity aspects that an organization complies with by implementing GDPR 10. Knowledge of incident management aspects that an organization complies with by implementing GDPR 11. Knowledge of how to establish an incident response plan based on the incident management process 12. Knowledge of the controls that need to be measured and monitored 13. Knowledge of when to monitor, measure, analyze and evaluate the performance of GDPR compliance project 14. Knowledge of who will monitor, measure, analyze and evaluate the performance of GDPR compliance project 15. Knowledge of how to monitor activities, processes and systems including incident management, physical and environmental security management, risk assessment process, security awareness and training, etc. 16. Knowledge of how to report the measurement results by using scorecards or strategic dashboards, tactical and operational dashboards, and reports and gauges 17. Knowledge of the main concepts related to continual improvement 18. Knowledge of how to continually monitor the change factors that influence the GDPR compliance project effectiveness

Based on the above-mentioned domains and their relevance, 12 questions are included in the exam, as summarized in the table below:

			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 the exam devoted to each competency domain	Number of points per competency domain	% of points per competency domain
Competency domains	Data protection concepts, general data protection regulation (GDPR), and compliance measures	10	X		5	41.7	30	40
		5	X					
		5		X				
		5	X					
		5		X				
	Roles and responsibilities of the data controllers, subcontractors, processors and the data protection officer (DPO)	10		X	2	16.6	15	20
		5	X					
	Technical and organizational measures for data protection	10	X		5	41.7	30	40
		5		X				
		5	X					
		5		X				
		5		X				
	Total points	75						
	Number of questions per level of understanding		6	6				
	% of the exam devoted to each level of understanding (cognitive/taxonomy)		50	50				

The passing score of the exam is **70%**.

After successfully passing the exam, candidates will be able to apply for the "PECB Certified Data Protection Officer" credential depending on their level of e

Taking the Exam

General Information on the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not be given additional time to compensate for the late arrival and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (a national ID card, driver's license, or passport) and show it to the invigilator.

If requested on the day of the exam (paper-based exams), additional time can be provided to candidates taking the exam in a non-native language, as follows:

- 10 additional minutes for Foundation exams
- 20 additional minutes for Manager exams
- 30 additional minutes for Lead exams

PECB Exam Format and Type

1. **Paper-based:** Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. The use of electronic devices, such as laptops, tablets, or phones, is not allowed. The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course.
2. **Online:** Exams are provided electronically via the PECB Exams application. The use of electronic devices, such as tablets and cell phones, is not allowed. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

For more detailed information about the online format, please refer to the PECB Online Exam Guide.

PECB exams are available in two types:
1. Essay-type question exam
2. Multiple-choice question exam

This exam comprises essay-type questions. They are used to determine and evaluate whether a candidate can clearly answer questions related to the defined competency domains. Additionally, problem-solving techniques and arguments that are supported with reasoning and evidence will also be evaluated.

The exam is open book and is not intended to measure memorizing or recalling information. It aims to evaluate candidates' comprehension, analytical skills, and applied knowledge. Therefore, candidates are required to provide logical and convincing answers and explanations in order to demonstrate that they have understood the content and the main concepts of the competency domains. You will find a sample of exam questions provided below.

Since the exam is "open book," candidates are authorized to use the following reference materials:
- A hard copy of the GDPR
- Training course materials (accessed through PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through PECB Exams app and/or printed)
- A hard copy dictionary

Any attempt to copy, collude, or otherwise cheat during the exam session will lead to automatic failure.

PECB exams are available in English and other languages. To learn if the exam is available in a particular language, please contact examination@pecb.com.

Note: PECB will progressively transition to multiple-choice exams. They will also be open book and comprise scenario-based questions that will allow PECB to evaluate candidates' knowledge, abilities, and skills to use information in new situations (apply), draw connections among ideas (analyze), and justify a stand or decision (evaluate). All PECB multiple-choice exams have one question and three alternatives, of which only one is correct.

For specific information about exam types, languages available, and other details, visit the List of PECB Exams.

Sample Exam Questions

Question 1: The purpose of 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 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.

Question 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 legislation
  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

Question 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*

Receiving the Exam Results

Exam results will be communicated via email.

- The time span for the communication starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

Candidates that disagree with the results may request a re-evaluation by writing to results@pecb.com within 30 days of receiving the results. Re-evaluation requests received after 30 days will not be processed. If candidates do not agree with the results of the reevaluation, they have 30 days from the date they received the reevaluated exam results to file a complaint through the PECB Ticketing System. Any complaint received after 30 days will not be processed.

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, s/he must wait 15 days after the initial date of the exam for the next attempt (1st retake).

  Note: Candidates who have completed the training course with one of our partners, and failed the first exam attempt, are eligible to retake for free the exam within a 12-month period from the date the coupon code is received, because the fee paid for the training course, includes a first exam attempt and one retake). Otherwise, retake fees apply.

For candidates that fail the exam retake, PECB recommends they attend a training course in order to be better prepared for the exam.

To arrange exam retakes, based on exam format, candidates that have completed a training course, must follow the steps below:

1. Online Exam: when scheduling the exam retake, use initial coupon code to waive the fee
2. Paper-Based Exam: candidates need to contact the PECB Partner/Distributor who has initially organized the session for exam retake arrangement (date, time, place, costs).

Candidates that have not completed a training course with a partner, but sat for the online exam directly with PECB, do not fall under this policy. The process to schedule the exam retake is the same as for the initial exam.

Exam Security

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams. Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals that violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Reschedule the Exam

For any changes with regard to the exam date, time, location, or other details, please contact examination@pecb.com.

Apply for Certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific educational and professional requirements need to be fulfilled in order to obtain a PECB certification. Candidates are required to fill out the online certification application form (that can be accessed via their PECB online profile), including contact details of references who will be contacted to validate the candidate's professional experience. Candidates can submit their application in various languages. Candidates can choose to either pay online or be billed. For additional information, contact certification@pecb.com.

The online certification application process is very simple and takes only a few minutes, as follows:

- Register your account
- Check your email for the confirmation link
- Log in to apply for certification

For more information about the application process, follow the instructions on this manual Apply for Certification.

The application is approved as soon as the Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. An email will be sent to the email address provided during the application process to communicate the application status. If approved, candidates will then be able to download the certification from their PECB Account.

PECB provides support in both English and French.

Renew your Certification

PECB certifications are valid for three years. To maintain them, candidates must demonstrate every year that they are still performing tasks that are related to the certification. PECB certified professionals must annually provide Continual Professional Development (CPD) credits and pay $120 as the Annual Maintenance Fee (AMF) to maintain the certification. For more information, please visit the Certification Maintenance page on the PECB website.

Closing a Case

If candidates do not apply for certification within three years, their case will be closed. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing and pay the required fee.

SECTION III: CERTIFICATION REQUIREMENTS

Certified Data Protection Officer

The requirements for PECB Certified Data Protection Officer certifications are:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Data Protection Officer	PECB Certified Data Protection Officer exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Data Protection Officer		Five years: Two years of work experience in data protection	Project activities: a total of 300 hours	Signing the PECB Code of Ethics

To be considered valid, the audit activities should follow best audit practices and include the following:

1. Assisting in applying the GDPR requirements
2. Monitoring a GDRP compliance program
3. Advising on the data protection impact assessment
4. Monitoring a data protection project with regard to the processing of personal data in alignment with the GDPR

PECB

SECTION IV: CERTIFICATION RULES AND POLICIES

Professional References

For each application, two professional references are required. They must be from individuals who have worked with the candidate in a professional environment and can validate their experience, as well as their current and previous work history. Professional references of persons who fall under the candidate's supervision or are their relatives are not valid.

Professional Experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the résumé.

Project Experience

The candidate's experience in data protection will be checked to ensure that the candidate has the required number of project experience hours.

Evaluation of Certification Applications

The Certification Department will evaluate each application to validate the candidate's eligibility for certification. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which can eventually lead to its downgrade to a lower credential.

Denial of Certification

PECB can deny certification if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics
- Fail the exam

For more detailed information, refer to "Complaint and Appeal" section.

The application payment for the certification is non-refundable.

Suspension of Certification

PECB can temporarily suspend certification if the candidate fails to satisfy the requirements. Other reasons for suspending certification include:

- PECB receives large amounts of or serious complaints by interested parties (Suspension will be applied until the investigation has been completed.).
- The logos of PECB or accreditation bodies are intentionally misused.
- The candidate fails to correct the misuse of a certification mark within the time frame determined by PECB.
- The certified individual has voluntarily requested a suspension.
- PECB deems appropriate other conditions for suspension of certification.

Revocation of Certification

PECB can revoke certification if the candidate fails to fulfill the PECB requirements. Candidates are then no longer allowed to represent themselves as PECB certified professionals. Other reasons for revoking certification can be if candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of the certification
- Break any other PECB rules

Upgrade of Credentials

Professionals can apply to upgrade to a higher credential as soon as they can demonstrate that they fulfil the requirements.

In order to apply for an upgrade, candidates need to login in to their PECB Account, visit the "My Certifications" tab, and click on the "Upgrade" link. The upgrade application fee is $100.

Downgrade of Credentials

A PECB Certification can be downgraded to a lower credential due to the following reasons:

- The AMF has not been paid.
- The CPD hours have not been submitted.
- Insufficient CPD hours have been submitted.
- Evidence on CPD hours has not been submitted upon request.

Note: *PECB certified professionals who hold Lead Certifications and fail to provide evidence of certification maintenance requirements will have their credentials downgraded. On the other hand, the holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. More information about these statuses and the permanent cessation status, and how to apply, please visit Certification Status Options.

PECB

SECTION V: PECB GENERAL POLICIES

PECB Code of Ethics

Adherence to the PECB Code of Ethics is a voluntary engagement. It is important that PECB certified professionals not only adhere to the principles of this Code, but also encourage and support the same from others. More information can be found here.

Other Exams and Certifications

PECB accepts certifications and exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective certification(s) or exam(s) can be accepted as equivalent to the respective PECB certification (e.g., ISO/IEC 27001 Lead Auditor certification).

Non-discrimination and Special Accommodations

All candidate applications will be evaluated objectively, regardless of the candidate's age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of a disability or a specific physical condition, they should inform the Partner/Distributor in order for them to make proper arrangements. Any information candidates provide regarding their disability/need will be treated with strict confidentiality.

Click here to download the Candidates with Disabilities Form.

Complaints and Appeals

Any complaints must be made no later than 30 days after receiving the certification decision. PECB will provide a written response to the candidate within 30 working days after receiving the complaint. If they do not find the response satisfactory, the candidate has the right to file an appeal. For more information about the complaints and appeal procedures, click here.

(1) According to ADA, the term "reasonable accommodation" may include: (A) making existing facilities used by employees readily accessible to and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.

(2) ADA Amendments Act of 2008 (P.L. 110-325) Sec. 12189. Examinations and courses. [Section 309]: Any person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or post-secondary education, professional, or trade purposes shall offer such examinations or courses in a place and manner accessible to persons with disabilities or offer alternative accessible arrangements for such individuals.

Address:
Headquarters
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax.
T: +1-844-426-7322
F: +1-844-329-7322

PECB Help Center
Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system.

Emails:
Examination: examination@pecb.com
Certification: certification@pecb.com
Customer Service: customer@pecb.com

Copyright © 2022 PECB. Reproduction or storage in any form for any purpose is not permitted without a PECB prior written permission.