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 resellers.

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 resellers who provide training courses and exam sessions. To find a training course provider in a particular region, candidates should go to Active Resellers. 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 resellers, 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 exam covers the following competency domain:

- **Domain 1:** Data protection concepts, General Data Protection Regulation (GDPR), and compliance measures
- **Domain 2:** Roles and responsibilities of accountable parties for the GDPR compliance
- **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 data protection concepts and principles and GDPR compliance measures	
Competencies	**Knowledge statements**
1. Ability to understand and explain the main data protection concepts and definitions 2. Ability to understand and interpret the GDPR objectives 3. Ability to understand, interpret, and analyze the GDPR requirements and structure 4. Ability to understand and explain the role of European Data Protection Board and other EU organizations 5. Ability to differentiate territorial and material scope, as defined in the GDPR 6. Ability to understand and interpret data protection principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality 7. Ability to understand the measures required to demonstrate compliance with the data protection principles 8. Ability to understand and interpret the rights of data subjects 9. Ability to understand the measures required to ensure compliance with data subject rights 10. Ability to understand the compliance measures required to protect data subject rights 11. Ability to understand the lawful basis for data processing	1. Knowledge of the main concepts and terminology of the GDPR 2. Knowledge of the GDPR objectives regarding the protection of natural persons 3. Knowledge of the GDPR requirements, including the GDPR articles and recitals 4. Knowledge of the concepts of material and territorial scope concepts provided by the GDPR, as well as their differences 5. Knowledge of the European Data Protection Board and other EU organizations, such as European Data Protection Supervisor, European Council, and European Commission 6. Knowledge of the role of the supervisory authority 7. Knowledge of how types of personal data are categorized and how they should be protected 8. Knowledge of the GDPR requirements for ensuring legitimate interest in data processing 9. Knowledge of the GDPR requirements for the processing of special categories of personal data 10. Knowledge of data protection principles 11. Knowledge of the rights of data subjects 12. Knowledge of challenges for achieving the GDPR compliance 13. Knowledge of the information that should be provided to the data subject for personal data processing 14. Knowledge of the GDPR requirements on the designation of a DPO

12. Ability to determine the information that shall be provided to data subjects for enabling them to exercise their rights 13. Ability to analyze and understand the GDPR compliance challenges 14. Ability to understand and interpret the role of the DPO 15. Ability to understand the GDPR requirements for organizations to design a DPO 16. Ability to analyze and understand the role of the controllers and processors under the GDPR 17. Ability to conduct and document a gap analysis 18. Ability to understand the internal and external environment of the organization 19. Ability to understand how the key processes and activities of the organization should be identified 20. Ability to evaluate and review a data protection policy and understand its importance 21. Ability to understand and identify processing activities 22. Ability to understand the importance of the DPO independence for achieving GDPR compliance 23. Ability to analyze the GDPR compliance program 24. Ability to identify the existence of data transfer outside the EU/EEA to third countries or international organizations	15. Knowledge of the qualifications of the DPO 16. Knowledge of the DPO employment contract 17. Knowledge of controllers, processors, and joint controllers concepts 18. Knowledge of the techniques used to gather information on an organization and to perform a gap analysis 19. Knowledge of how maturity levels should be established and their applicability 20. Knowledge of the best practices and techniques used to draft and establish data protection policies and procedures 21. Knowledge of records of processing activities and their importance 22. Knowledge of the GDPR requirements for recording processing activities 23. Knowledge of mechanisms that should be used for transfers of data outside EU/EEA to third countries or international organizations 24. Knowledge of the UK's implementation of GDPR and the differences between the UK GDPR and EU GDPR

PECB

Domain 2: Roles and responsibilities of accountable parties for the GDPR compliance

Main objective: Ensure that the candidate understands and is able to interpret the roles and responsibilities of all accountable parties for achieving GDPR compliance

Competencies	Knowledge statements
1. Ability to understand the role and responsibilities of the DPO 2. Ability to understand and interpret the GDPR requirements for the position of the DPO 3. Ability to understand the role, responsibilities, and obligations of the controller and the processor under the GDPR 4. Ability to understand the role of the controller in implementing adequate measures for GDPR compliance, such as data protection by design and data protection by default 5. Ability to understand the role of joint controllers according to the GDPR 6. Ability to understand the role of the controller and processor regarding the cooperation with the supervisory authority 7. Ability to understand the role of the top management of the organization in the GDPR implementation 8. Ability to define the obligations of the controller regarding data protection 9. Ability to understand the role of the controller, processor, and DPO in keeping records of processing activities 10. Ability to understand and interpret the role of the DPO in ensuring GDPR compliance for transfers to international organizations and third countries 11. Ability to understand the role of the DPO in identifying, analyzing, evaluating, and treating data protection risks 12. Ability to understand the recording process of processing activities 13. Ability to create and maintain records of processing activities	1. Knowledge of the role of the controller and processor in data processing 2. Knowledge of the role and obligations of joint controllers in data processing 3. Knowledge of the role and responsibilities of the DPO in the GDPR compliance program 4. Knowledge of the controller and processor general obligations according to the GDPR 5. Knowledge of the DPIA process and its importance 6. Knowledge of the role of the DPO in the DPIA 7. Knowledge of the differences between risk assessment and DPIA 8. Knowledge of cases when the DPIA is necessary according to the GDPR 9. Knowledge of information flow mapping 10. Knowledge of data protection solutions 11. Knowledge of different DPIA methodologies, including CNIL and ICO 12. Knowledge of the DPO role on documentation management 13. Knowledge of how documented information should be created and maintained to ensure GDPR compliance 14. Knowledge of the different approaches and methodologies used to perform risk assessment 15. Knowledge of the role of the DPO in data protection risk management 16. Knowledge of records of processing activities and their importance 17. Knowledge of how processing activities should be recorded based on the GDPR 18. Knowledge of incident management standards and industry best practices 19. Knowledge of incident management phases, including plan and prepare, detection and

14. Ability to understand the role of the DPO in a data protection impact assessment (DPIA) 15. Ability to understand the iterative process for conducting a DPIA 16. Ability to conduct and provide advice on the DPIA 17. Ability to understand and define the need for a DPIA 18. Ability to understand how the information flow should be mapped 19. Ability to understand data protection solutions and select an appropriate solution for the identified risks 20. Ability to understand and identify various DPIA methodologies 21. Ability to create and maintain documented information 22. Ability to understand the role of the DPO in incident management and personal data breaches 23. Ability to understand the role of the data controller, processor, and supervisory authority in incident management and personal data breaches 24. Ability to understand the incident management process 25. Ability to draft a resolution report as part of the personal data breach response plan 26. Ability to identify personal data breaches that require the notification of the supervisory authority 27. Ability to identify personal data breaches that shall be communicated to the data subjects 28. Ability to understand the role of the DPO and the controller in notification of a personal data breach	reporting, assessment and decision, responses, and lessons learnt 20. Knowledge on how to detect, respond to, and report incidents and personal data breaches 21. Knowledge of personal data breaches and personal data breach response plan 22. Knowledge of measures that should be taken to respond to a personal data breach, including containment and eradication 23. Knowledge of resolution report of a personal data breach 24. Knowledge of personal data breaches that shall be communicated to data subjects 25. Knowledge of personal data breaches that shall be communicated to the supervisory authority 26. Knowledge of the GDPR requirements regarding the period of notification of data subjects and supervisory authority in case of a personal data breach 27. Knowledge of what a personal data breach notification to the supervisory authority shall include 28. Knowledge of the information that shall be provided to the data subjects in case of a personal data breach

PECB

Domain 3: Technical and organizational measures for data protection

Main objective: Ensure that the candidate is able to determine the necessary technical and organizational measures to ensure protection of personal data being processed

Competencies

1. Ability to understand and explain the concepts of data protection by design and by default
2. Ability to understand and identify de-identification methods and techniques to protect personal data
3. Ability to understand and interpret the differences between anonymization and pseudonymization
4. Ability to understand the implementation of security measures, such as access controls and logging and monitoring to ensure data protection
5. Ability to define and implement appropriate data protection training and awareness programs and communication plans
6. Ability to establish a communication plan to assist in the understanding of an organization's data protection issues, policies, and performance
7. Ability to monitor and evaluate the effectiveness of the GDPR compliance program
8. Ability to verify to what extent the identified GDPR compliance program objectives have been met
9. Ability to define and implement a data protection internal audit program
10. Ability to perform regular and methodical reviews to ensure the suitability, adequacy, effectiveness, and efficiency of the GDPR compliance program based on the policies and objectives of the organization
11. Ability to understand the concept of a data protection external audit
12. Ability to track and take action on nonconformities

Knowledge statements

1. Knowledge of the objectives and measures of data protection by design and by default
2. Knowledge of how anonymization and psydonymization techniques should be implemented
3. Knowledge of the technical security measures that ensure data protection and their implementation
4. Knowledge of how personal data should be protected when using mobile and portable devices
5. Knowledge of the characteristics and the best practices of implementing data protection training and awareness programs and communication plans
6. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence
7. Knowledge of the best practices and techniques used to monitor and evaluate the effectiveness of the GDPR compliance program
8. Knowledge of the concepts related to measurement and evaluation
9. Knowledge of the main concepts and components related to the implementation and operation of a data protection internal audit
10. Knowledge of the difference between a major and a minor nonconformity
11. Knowledge of the guidelines and best practices to draft a nonconformity report
12. Knowledge of the main processes, tools, and techniques used to identify the root causes of nonconformities
13. Knowledge of the treatment of nonconformities process

13. Ability to identify and analyze the root causes of nonconformities and propose action plans to treat them 14. Ability to advise an organization on how to continually improve the effectiveness and efficiency of a GDPR compliance program 15. Ability to implement continual improvement processes in an organization 16. Ability to determine the appropriate tools to support the continual improvement processes of an organization	14. Knowledge of the main processes, tools, and techniques used to develop corrective action plans 15. Knowledge of the main concepts related to continual improvement 16. Knowledge of the processes related to the continual monitoring of change factors 17. Knowledge of the maintenance and improvement of a GDPR compliance program

Based on the abovementioned domains and their relevance, 80 questions are included in the exam, as summarized in the table below:

				Level of understanding (Cognitive/Taxonomy) required	
		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Questions that measure comprehension, application, and analysis	Questions that measure synthesis and evaluation
Competency domains	Data protection concepts, General Data Protection Regulation (GDPR), and compliance measures	40	50	X	
	Roles and responsibilities of accountable parties for the GDPR compliance	25	31.25		X
	Technical and organizational measures for data protection	15	18.75		X
	Total	**80**	**100%**		
	Number of questions per level of understanding			**40**	**40**
	% 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 experience.

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 Reseller 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.

This exam contains multiple choice questions: This format has been chosen because it has proven to be effective and efficient for measuring and assessing learning outcomes related to the defined competency domains. The multiple-choice exam can be used to evaluate a candidate's understanding on many subjects, including both simple and complex concepts. When answering these questions, candidates will have to apply various principles, analyze problems, evaluate alternatives, combine several concepts or ideas, etc. The multiple-choice questions are scenario based, which means they are developed based on a scenario that candidates are asked to read and are expected to provide answers to one or more questions related to that scenario. This multiple-choice exam is "open book", due to the context-dependent characteristic of the questions. 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 during the training course (accessed through the 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

Scenario:

Matix is a French company that provides software development services. The company was found in 2016 and works with many businesses across Europe. *Matix*'s teams mostly develop mobile applications and custom software solutions. The last project that *Matix*'s developers have been working on is the development of *AskME*, a survey cross-platform that can be used for both iOS and Android. It offers a simple way for creating online surveys and it is one of the most popular apps in Europe with more than 35 million European users. An automated data analysis solution has also been integrated into the application to analyze answers. Typically, a survey form created in *AskME* requires the name, surname, and email address of the respondent. The creator of the survey may require additional information by adding other fields in the form. Prior to collecting data, *AskME* provides information to users on how the data is collected and the purpose of collection.

Last month, *Matix* revealed that they experienced a security incident that exposed the names and surnames of about a thousand respondents. After an internal investigation, the company found out that a group of hackers had taken advantage of a vulnerability in their survey application. They stated that the information that was accessed by hackers belonged to *AskME* users.

Based on this scenario, answer the following questions:

1. **Why should *Matix* comply with the GDPR?**
   A. Because the GDPR applies to all European organizations, regardless of their nature of operations
   B. **Because *Matix*'s activities involve processing of personal data of EU residents wholly or partly by automated means**
   C. Because *Matix* experienced a security incident which exposed the names and surnames of about a thousand people

2. **Which right of data subjects does *Matix* ensure by enabling *AskME*'s users to know the purpose of collection?**
   A. **Right to be informed**
   B. Right to access
   C. Right to restriction of processing

3. **What should *Matix* do to avoid similar incidents in the future?**
   A. **Use pseudonymization techniques to ensure that personal data cannot be linked to a natural person**
   B. Use anonymization techniques to ensure that the name, surname, and email address cannot be retrieved
   C. Stop the processing of clients' personal data to preserve their anonymity

4. **Should *Matix* clients be notified about the incident described in the scenario?**
   A. No, the personal data belonged to users of *AskME*, who are not direct clients of *Matix*
   B. No, the incident exposed only the name and surname of clients
   C. **Yes, the incident resulted in a personal data breach**

Receiving the Exam Results

Exam results will be communicated via email. The only possible results are *pass* and *fail*; no specific grade will be included.

- The time span for the communication starts from the exam date and lasts 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.

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 allowed time span between exam retakes.

- If a candidate does not pass the exam on the 1st attempt, they must wait 15 days from the initial date of the exam for the next attempt (1st retake). Retake fees apply.
  Note: *Candidates who have completed the training course but failed the 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 2nd attempt, they must wait three months after the initial date of the exam for the next attempt (2nd retake). Retake fees apply.
  Note: For candidates that fail the exam in the 2nd retake, PECB recommends them to attend a training course in order to be better prepared for the exam.
- If a candidate does not pass the exam on the 3rd attempt, they must wait six months after the initial date of the exam for the next attempt (3rd retake). Retake fees apply.
- After the 4th attempt, the waiting period for further retake exams is 12 months from the date of the last attempt. Retake fees apply.

To arrange exam retakes (date, time, place, costs), candidates need to contact the PECB Reseller/Distributor who has initially organized the session.

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 $100 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 activities should follow best data protection 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

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 Reseller/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