PECB

BEYOND RECOGNITION

CERTIFIED DATA PROTECTION OFFICER

Candidate Handbook

PECB

Table of Contents

PECB

SECTION I: INTRODUCTION

About PECB

PECB is a certification body that provides education[1], certification, and certificate programs for individuals on a wide range of disciplines.

Through our presence in more than 150 countries, we help professionals demonstrate their competence in various areas of expertise by providing valuable evaluation, certification, and certificate programs against internationally recognized standards.

Our key objectives are:

1. Establishing the minimum requirements necessary to certify professionals and to grant designations
2. Reviewing and verifying the qualifications of individuals to ensure they are eligible for certification
3. Maintaining and continually improving the evaluation process for certifying individuals
4. Certifying qualified individuals, granting designations and maintaining respective directories
5. Establishing requirements for the periodic renewal of certifications and ensuring that the certified individuals are complying with those requirements
6. Ascertaining that PECB professionals meet ethical standards in their professional practice
7. Representing our stakeholders in matters of common interest
8. Promoting the benefits of certification and certificate programs to professionals, businesses, governments, and the public

Our mission

Provide our clients with comprehensive examination, certification, and certificate program services that inspire trust and benefit the society as a whole.

Our vision

Become the global benchmark for the provision of professional certification services and certificate programs.

Our values

Integrity, Professionalism, Fairness

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

The Value of PECB Certification

Global recognition
PECB credentials are internationally recognized and endorsed by many accreditation bodies, so professionals who pursue them will benefit from our recognition in domestic and international markets.

The value of PECB certifications is validated by the accreditation from the International Accreditation Service (IAS-PCB-111), the United Kingdom Accreditation Service (UKAS-No. 21923) and the Korean Accreditation Board (KAB-PC-08) under ISO/IEC 17024 – General requirements for bodies operating certification of persons. The value of PECB certificate programs is validated by the accreditation from the ANSI National Accreditation Board (ANAB-Accreditation ID 1003) under ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB is an associate member of The Independent Association of Accredited Registrars (IAAR), a full member of the International Personnel Certification Association (IPC), a signatory member of IPC MLA, and a member of Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine, and ITCC. In addition, PECB is an approved Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC), is approved by Club EBIOS to offer the EBIOS Risk Manager Skills certification, and is approved by CNIL (Commission Nationale de l'Informatique et des Libertés) to offer DPO certification. For more detailed information, click here.

High-quality products and services
We are proud to provide our clients with high-quality products and services that match their needs and demands. All of our products are carefully prepared by a team of experts and professionals based on the best practices and methodologies.

Compliance with standards
Our certifications and certificate programs are a demonstration of compliance with ISO/IEC 17024 and ASTM E2659. They ensure that the standard requirements have been fulfilled and validated with adequate consistency, professionalism, and impartiality.

Customer-oriented service
We are a customer-oriented company and treat all our clients with value, importance, professionalism, and honesty. PECB has a team of experts who are responsible for addressing requests, questions, and needs. We do our best to maintain a 24-hour maximum response time without compromising the quality of the services.

Flexibility and convenience
Online learning opportunities make your professional journey more convenient as you can schedule your learning sessions according to your lifestyle. Such flexibility gives you more free time, offers more career advancement opportunities, and reduces costs.

PECB Code of Ethics

The Code of Ethics represents the highest values and ethics that PECB is fully committed to follow, as it recognizes the importance of them when providing services and attracting clients.

The Compliance Division makes sure that PECB employees, trainers, examiners, invigilators, partners, distributors, members of different advisory boards and committees, certified individuals, and certificate holders (hereinafter "PECB professionals") adhere to this Code of Ethics. In addition, the Compliance Division consistently emphasizes the need to behave professionally and with full responsibility, competence, and fairness in service provision with internal and external stakeholders, such as applicants, candidates, certified individuals, certificate holders, accreditation authorities, and government authorities.

It is PECB's belief that to achieve organizational success, it has to fully understand the clients and stakeholders' needs and expectations. To do this, PECB fosters a culture based on the highest levels of integrity, professionalism, and fairness, which are also its values. These values are integral to the organization, and have characterized the global presence and growth over the years and established the reputation that PECB enjoys today.

PECB believes that strong ethical values are essential in having healthy and strong relationships. Therefore, it is PECB's primary responsibility to ensure that PECB professionals are displaying behavior that is in full compliance with PECB principles and values.

PECB professionals are responsible for:

1. Displaying professional behavior in service provision with honesty, accuracy, fairness, and independence
2. Acting at all times in their service provision solely in the best interest of their employer, clients, the public, and the profession in accordance with this Code of Ethics and other professional standards
3. Demonstrating and developing competence in their respective fields and striving to continually improve their skills and knowledge
4. Providing services only for those that they are qualified and competent and adequately informing clients and customers about the nature of proposed services, including any relevant concerns or risks
5. Informing their employer or client of any business interests or affiliations which might influence or impair their judgment
6. Preserving the confidentiality of information of any present or former employer or client during service provision
7. Complying with all the applicable laws and regulations of the jurisdictions in the country where the service provisions were conducted
8. Respecting the intellectual property and contributions of others
9. Not communicating intentionally false or falsified information that may compromise the integrity of the evaluation process of a candidate for a PECB certification or a PECB certificate program
10. Not falsely or wrongly presenting themselves as PECB representatives without a proper license or misusing PECB logo, certifications or certificates
11. Not acting in ways that could damage PECB's reputation, certifications or certificate programs
12. Cooperating in a full manner on the inquiry following a claimed infringement of this Code of Ethics

To read the complete version of PECB's Code of Ethics, go to Code of Ethics | PECB.

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.

PECB certifications are not a license or simply a membership. They attest the candidates' knowledge and skills gained through our training courses and are issued to candidates that have the required experience and have passed the exam.

This document specifies the PECB Certified Data Protection Officer certification scheme in compliance with ISO/IEC 17024:2012. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your application. If you have questions or need further information after reading it, please contact the PECB international office at certification.team@pecb.com.

PECB

SECTION II: EXAMINATION PREPARATION, RULES, AND POLICIES

Preparing for and scheduling the exam

All candidates are responsible for their own study and preparation for certification exams. Although candidates are not required to attend the training course to be eligible for taking the exam, attending it can significantly increase their chances of successfully passing the exam.

To schedule the exam, candidates have two options:

1. Contact one of our authorized partners. To find an authorized partner in your region, please go to Active Partners. The training course schedule is also available online and can be accessed on Training Events.
2. Take a PECB exam remotely through the PECB Exams application. To schedule a remote exam, please go to the following link: Exam Events.

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

Rescheduling the exam

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

Application fees for examination and certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: $1000[2]
- Manager Exam: $700
- Foundation Exam: $500
- Transition Exam: $500

The application fee for certification is $500.

For the candidates that have attended the training course via one of PECB's partners, the application fee covers the costs of the exam (first attempt and first retake), the application for certification, and the first year of Annual Maintenance Fee (AMF).

[2] All prices listed in this document are in US dollars.

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 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	1. Knowledge of the main concepts and terminology of the GDPR
2. Ability to understand and interpret the GDPR objectives	2. Knowledge of the GDPR objectives regarding the protection of natural persons
3. Ability to understand, interpret, and analyze the GDPR requirements and structure	3. Knowledge of the GDPR requirements, including the GDPR articles and recitals
4. Ability to understand and explain the role of European Data Protection Board and other EU organizations	4. Knowledge of the concepts of material and territorial scope concepts provided by the GDPR, as well as their differences
5. Ability to differentiate territorial and material scope, as defined in the GDPR	5. Knowledge of the European Data Protection Board and other EU organizations, such as European Data Protection Supervisor, European Council, and European Commission
6. Ability to understand and interpret data protection principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality	6. Knowledge of the role of the supervisory authority
7. Ability to understand the measures required to demonstrate compliance with the data protection principles	7. Knowledge of how types of personal data are categorized and how they should be protected
8. Ability to understand and interpret the rights of data subjects	8. Knowledge of the GDPR requirements for ensuring legitimate interest in data processing
9. Ability to understand the measures required to ensure compliance with data subject rights	9. Knowledge of the GDPR requirements for the processing of special categories of personal data
10. Ability to understand the compliance measures required to protect data subject rights	10. Knowledge of data protection principles
11. Ability to understand the lawful basis for data processing	11. Knowledge of the rights of data subjects
12. Ability to determine the information that shall be provided to data subjects for enabling them to exercise their rights	12. Knowledge of challenges for achieving the GDPR compliance
13. Ability to analyze and understand the GDPR compliance challenges	13. Knowledge of the information that should be provided to the data subject for personal data processing
14. Ability to understand and interpret the role of the DPO	14. Knowledge of the GDPR requirements on the designation of a DPO
15. Ability to understand the GDPR requirements for organizations to design a DPO	15. Knowledge of the qualifications of the DPO
	16. Knowledge of the DPO employment contract
	17. Knowledge of controllers, processors, and joint controllers concepts

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	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

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	1. Knowledge of the role of the controller and processor in data processing
2. Ability to understand and interpret the GDPR requirements for the position of the DPO	2. Knowledge of the role and obligations of joint controllers in data processing
3. Ability to understand the role, responsibilities, and obligations of the controller and the processor under the GDPR	3. Knowledge of the role and responsibilities of the DPO in the GDPR compliance program
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	4. Knowledge of the controller and processor general obligations according to the GDPR
5. Ability to understand the role of joint controllers according to the GDPR	5. Knowledge of the DPIA process and its importance
6. Ability to understand the role of the controller and processor regarding the cooperation with the supervisory authority	6. Knowledge of the role of the DPO in the DPIA
7. Ability to understand the role of the top management of the organization in the GDPR implementation	7. Knowledge of the differences between risk assessment and DPIA
8. Ability to define the obligations of the controller regarding data protection	8. Knowledge of cases when the DPIA is necessary according to the GDPR
9. Ability to understand the role of the controller, processor, and DPO in keeping records of processing activities	9. Knowledge of information flow mapping
10. Ability to understand and interpret the role of the DPO in ensuring GDPR compliance for transfers to international organizations and third countries	10. Knowledge of data protection solutions
11. Ability to understand the role of the DPO in identifying, analyzing, evaluating, and treating data protection risks	11. Knowledge of different DPIA methodologies, including CNIL and ICO
12. Ability to understand the recording process of processing activities	12. Knowledge of the DPO role on documentation management
13. Ability to create and maintain records of processing activities	13. Knowledge of how documented information should be created and maintained to ensure GDPR compliance
14. Ability to understand the role of the DPO in a data protection impact assessment (DPIA)	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

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

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	Knowledge statements
1. Ability to understand and explain the concepts of data protection by design and by default	1. Knowledge of the objectives and measures of data protection by design and by default
2. Ability to understand and identify de-identification methods and techniques to protect personal data	2. Knowledge of how anonymization and psydonymization techniques should be implemented
3. Ability to understand and interpret the differences between anonymization and pseudonymization	3. Knowledge of the technical security measures that ensure data protection and their implementation
4. Ability to understand the implementation of security measures, such as access controls and logging and monitoring to ensure data protection	4. Knowledge of how personal data should be protected when using mobile and portable devices
5. Ability to define and implement appropriate data protection training and awareness programs and communication plans	5. Knowledge of the characteristics and the best practices of implementing 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	6. Knowledge of the communication objectives, activities, and interested parties to enhance their support and confidence
7. Ability to monitor and evaluate the effectiveness of the GDPR compliance program	7. Knowledge of the best practices and techniques used 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	8. Knowledge of the concepts related to measurement and evaluation
9. Ability to define and implement a data protection internal audit program	9. Knowledge of the main concepts and components related to the implementation and operation of a data protection internal audit
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	10. Knowledge of the difference between a major and a minor nonconformity
11. Ability to understand the concept of a data protection external audit	11. Knowledge of the guidelines and best practices to draft a nonconformity report
12. Ability to track and take action on nonconformities	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 above-mentioned domains and their relevance, the exam contains 80 multiple-choice questions, 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 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 obtaining the "PECB Certified Data Protection Officer" credential.

Taking the exam

General information about 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 information about online exams, go 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 multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding on both simple and complex concepts. It comprises both stand-alone and scenario-based questions. Stand-alone questions stand independently within the exam and are not context-depended, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario which a candidate is asked to read and is expected to provide answers to five questions related to that scenario. When answering stand-alone and scenario-based questions, candidates will have to apply various concepts and principles explained during the training course, analyze problems, identify and evaluate alternatives, combine several concepts or ideas, etc.

Each multiple-choice question has three options, of which one is the correct response option (keyed response) and two incorrect response options (distractors).

This is an open-book exam. The candidate is allowed to use the following reference materials:

- A hard copy of the GDPR
- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

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).

For specific information about exam types, languages available, and other details, please contact examination.team@pecb.com or go to the List of PECB Exams.

Sample exam questions

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

Exam Security Policy

PECB is committed to protect the integrity of its exams and the overall examination process, and relies upon the ethical behavior of applicants, potential applicants, candidates and partners to maintain the confidentiality of PECB exams. This Policy aims to address unacceptable behavior and ensure fair treatment of all candidates.

Any disclosure of information about the content of PECB exams is a direct violation of this Policy and PECB's Code of Ethics. Consequently, candidates taking a PECB exam are required to sign an Exam Confidentiality and Non-Disclosure Agreement and must comply with the following:

1. The questions and answers of the exam materials are the exclusive and confidential property of PECB. Once candidates complete the submission of the exam to PECB, they will no longer have any access to the original exam or a copy of it.
2. Candidates are prohibited from revealing any information regarding the questions and answers of the exam or discuss such details with any other candidate or person.
3. Candidates are not allowed to take with themselves any materials related to the exam, out of the exam room.
4. Candidates are not allowed to copy or attempt to make copies (whether written, photocopied, or otherwise) of any exam materials, including, without limitation, any questions, answers, or screen images.
5. Candidates must not participate nor promote fraudulent exam-taking activities, such as:
    - Looking at another candidate's exam material or answer sheet
    - Giving or receiving any assistance from the invigilator, candidate, or anyone else
    - Using unauthorized reference guides, manuals, tools, etc., including using "brain dump" sites as they are not authorized by PECB

Once a candidate becomes aware or is already aware of the irregularities or violations of the points mentioned above, they are responsible for complying with those, otherwise if such irregularities were to happen, candidates will be reported directly to PECB or if they see such irregularities, they should immediately report to PECB.

Candidates are solely responsible for understanding and complying with PECB Exam Rules and Policies, Confidentiality and Non-Disclosure Agreement and Code of Ethics. Therefore, should a breach of one or more rules be identified, candidates will not receive any refunds. In addition, PECB has the right to deny the right to enter a PECB exam or to invite candidates for an exam retake if irregularities are identified during and after the grading process, depending on the severity of the case.

Any violation of the points mentioned above will cause PECB irreparable damage for which no monetary remedy can make up. Therefore, PECB can take the appropriate actions to remedy or prevent any unauthorized disclosure or misuse of exam materials, including obtaining an immediate injunction. PECB will take action against individuals that violate the rules and policies, including permanently banning them 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.

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 examination.team@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, they 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 (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.

PECB

SECTION III: CERTIFICATION PROCESS AND REQUIREMENTS

Certified Data Protection Officer credentials

All PECB certifications have specific requirements regarding education and professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB CDPO scheme have the following requirements:

Credential	Education	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Data Protection Officer	At least secondary education	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	

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

Applying for certification

All candidates who successfully pass the exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credential they were assessed 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 account), including contact details of individuals who will be contacted to validate the candidates' professional experience. Candidates can submit their application in English, French, German, Spanish or Korean languages. They can choose to either pay online or be billed. For additional information, please contact certification.team@pecb.com.

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

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

For more information on how to apply for certification, click here.

The Certification Department validates that the candidate fulfills all the certification requirements regarding the respective credential. The candidate will receive an email about the application status, including the certification decision.

Following the approval of the application by the Certification Department, the candidate will be able to download the certificate and claim the corresponding Digital Badge. For more information about downloading the certificate, click here, and for more information about claiming the Digital Badge, click here.

PECB provides support both in English and French.

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.

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.

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 candidates' eligibility for certification or certificate program. 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 may lead to the candidates' credential downgrade.

SECTION IV: CERTIFICATION POLICIES

Denial of certification

PECB can deny certification/certificate program if candidates:

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

Candidates whose certification/certificate program has been denied can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

The application payment for the certification/certificate program is nonrefundable.

Certification status options

Active

Means that your certification is in good standing and valid, and it is being maintained by fulfilling the PECB requirements regarding the CPD and AMF.

Suspended

PECB can temporarily suspend candidates' certification if they fail to meet the requirements. Other reasons for suspending certification include:

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

Revoked

PECB can revoke (that is, to withdraw) the certification if the candidate fails to satisfy its requirements. In such cases, candidates are no longer allowed to represent themselves as PECB Certified Professionals. Additional reasons for revoking certification can be if the candidates:

- Violate the PECB Code of Ethics
- Misrepresent and provide false information of the scope of certification
- Break any other PECB rules
- Any other reasons that PECB deems appropriate

Candidates whose certification has been revoked can file a complaint through the complaints and appeals procedure. For more detailed information, refer to **Complaint and Appeal Policy** section.

Other statuses
Besides being active, suspended, or revoked, a certification can be voluntarily withdrawn or designated as Emeritus. To learn more about these statuses and the permanent cessation status, go to Certification Status Options.

Upgrade and downgrade of credentials

Upgrade of credentials
Professionals can upgrade their credentials as soon as they can demonstrate that they fulfill the requirements.

To apply for an upgrade, candidates need to log into their PECB account, visit the "My Certifications" tab, and click on "Upgrade." 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. The holders of Master Certifications who fail to submit CPDs and pay AMFs will have their certifications revoked.*

Renewing the certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continual professional development (CPD) hours. In addition, they need to pay the annual maintenance fee ($120). For more information, go to the Certification Maintenance page on the PECB website.

Closing a case

If candidates do not apply for certification within one year, 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 to certification.team@pecb.com and pay the required fee.

Complaint and Appeal Policy

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 candidates do not find the response satisfactory, they have the right to file an appeal.

For more information about the Complaint and Appeal Policy, click here.

PECB

SECTION V: GENERAL POLICIES

Exams and certifications from other accredited certification bodies

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 candidates' age, gender, race, religion, nationality, or marital status.

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations[3] 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[4]. Any information that candidates provide regarding their disability/special needs will be treated with confidentiality. To download the Candidates with Disabilities Form, click here.

Behavior Policy

PECB aims to provide top-quality, consistent, and accessible services for the benefit of its external stakeholders: distributors, partners, trainers, invigilators, examiners, members of different committees and advisory boards, and clients (trainees, examinees, certified individuals, and certificate holders), as well as creating and maintaining a positive work environment which ensures safety and well-being of its staff, and holds the dignity, respect and human rights of its staff in high regard.

The purpose of this Policy is to ensure that PECB is managing unacceptable behavior of external stakeholders towards PECB staff in an impartial, confidential, fair, and timely manner. To read the Behavior Policy, click here.

Refund Policy

PECB will refund your payment, if the requirements of the Refund Policy are met. To read the Refund Policy, click here.

[3] 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.

[4] 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

Emails:

Examination:
examination.team@pecb.com

Certification:
certification.team@pecb.com

Customer Service:
support@pecb.com

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.

www.pecb.com