



PECB

Candidate Handbook

CERTIFIED U.S. DATA PRIVACY
OFFICER

Contents

SECTION I: INTRODUCTION.....	3
About PECB	3
Accreditations and Affiliations	3
PECB Code of Ethics.....	3
Introduction to Certified U.S. Data Privacy Officer Certification.....	4
SECTION II: EXAM PROCESS, RULES AND POLICIES	5
Preparing For and Scheduling the Exam.....	5
Special Accommodations.....	5
Taking the Exam.....	5
Exam Results.....	6
Exam Retake Policy.....	6
Exam Security Policy	6
Exam Competency Domains	7
Sample Exam Questions.....	16
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES	18
PECB Certified U.S. Data Privacy Officer Credentials	18
Applying for Certification	18
Professional Experience	19
Professional References	19
Project Experience	19
Evaluation of Certification Applications.....	19
SECTION IV: CERTIFICATION MAINTENANCE POLICY	20
Renewing the Certification	20
Upgrade Credentials.....	20
Suspension of Certification	20
Revocation of Certification.....	20
Other Statuses.....	20
SECTION V: OTHER POLICIES	21
Application Fees for Examination and Certification	21
Complaint and Appeal Policy	21
Exams from Other Accredited Certification Bodies.....	21
Refund Policy.....	21

SECTION I: INTRODUCTION

About PECB¹

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Vision: As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission: Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values: Growth, Change, Harmony, Simplicity, Reliability, and Quality

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click [here](#).

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, and defines the responsibilities of PECB professionals, including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals, and certificate holders. To read the PECB's Code of Ethics, click [here](#).

¹ Notes:

- The legal name of PECB is "PECB Group Pte. Ltd."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024. Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to Certified U.S. Data Privacy Officer Certification

This document specifies the PECB Certified U.S. Data Privacy Officer scheme in compliance with ISO/IEC 17024. 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 certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking [here](#).

Preparing For and Scheduling the Exam

To schedule the exam, candidates have two options:

1. **Online:** Through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and location where the candidate is going to attend the exam.

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

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the [myPECB](#) dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

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

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

Online Exam Rules	Paper-Based Exam Rules
• Exams are provided electronically via the PECB Exams application. • The use of secondary electronic devices, such as tablets and phones, is not allowed during the exam. • The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera. • If requested on the day of the exam, 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	• 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. • If requested on the day of the exam, 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

For specific information on exam types, languages available, and other details, please check the [List of PECB Exams](#).

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results 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.

If candidates disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

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. For more information, please visit this link: [Exam Rules and Policies - PECB](#).

Exam Security Policy

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 who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Privacy foundations and regulatory framework

Main objective: Ensure that the candidate is able to interpret and discuss foundational privacy principles and regulatory frameworks governing personal data protection across the United States and key international jurisdictions.

Competencies	Knowledge statements
1. Ability to interpret legal terminology and constitutional concepts relevant to privacy and personal data protection 2. Ability to explain the hierarchy of legal authority in the U.S. and its impact on privacy regulation 3. Ability to identify and interpret federal privacy laws and regulatory mechanisms governing personal data in the U.S. 4. Ability to analyze the role and enforcement authority of regulatory bodies responsible for privacy oversight in the U.S. 5. Ability to assess regulatory obligations related to financial data protection 6. Ability to recognize regulatory developments affecting international access to personal data held in the U.S. 7. Ability to evaluate the scope and applicability of U.S. state privacy laws and related compliance requirements 8. Ability to recognize and compare global data protection frameworks across different jurisdictions 9. Ability to analyze regional approaches to data protection in Europe, the Asia-Pacific region, Africa, and the United Kingdom 10. Ability to define and interpret key data privacy concepts and terminology within regulatory and organizational contexts 11. Ability to apply fundamental privacy principles in the governance and protection of personal data	1. Knowledge of U.S. legal and constitutional terms related to privacy and data protection 2. Knowledge of the hierarchy of legal authority in the U.S., including constitutional provisions, federal statutes, regulations, and state laws 3. Knowledge of federal privacy laws and regulations in the U.S. 4. Knowledge of the role and authority of the Federal Trade Commission (FTC). 5. Knowledge of the Gramm-Leach-Bliley Act and the FTC Safeguards Rule 6. Knowledge of Executive Order 14117 and the associated Final Rule 7. Knowledge of U.S. state privacy laws and associated consumer rights and organizational obligations 8. Knowledge of data protection laws and privacy frameworks worldwide 9. Knowledge of major regional data protection laws in Europe, Asia-Pacific, Africa, and the United Kingdom 10. Knowledge of data privacy concepts, definitions in the U.S. context, and environments of data protection 11. Knowledge of the Fair Information Practice Principles (FIPPs)

Domain 2: Privacy governance, leadership, and organizational roles

Main objective: Ensure that the candidate is able to explain privacy governance structures, leadership responsibilities, and organizational roles necessary to support effective privacy compliance and data protection programs.

Competencies	Knowledge statements
1. Ability to explain the principles and objectives of privacy leadership and governance within organizations	1. Knowledge of data protection leadership principles and governance approaches for privacy management
2. Ability to integrate privacy values and data protection principles into organizational operations and decision-making processes	2. Knowledge of approaches for integrating privacy values into organizational operations and decision-making
3. Ability to promote privacy culture, awareness, and training initiatives within an organization	3. Knowledge of strategies for promoting organizational privacy culture, awareness, and training programs
4. Ability to manage privacy compliance programs and contractual privacy requirements across business operations	4. Knowledge of privacy compliance management and contractual privacy requirements within organizations
5. Ability to interpret regulatory requirements and translate them into operational privacy controls and policies	5. Knowledge of regulatory interpretation and implementation processes for privacy and data protection requirements
6. Ability to oversee third-party privacy obligations, contractual requirements, and vendor risk management processes	6. Knowledge of third-party privacy obligations, contractual requirements, and vendor risk management practices
7. Ability to evaluate organizational privacy governance models, including centralized and decentralized privacy structures	7. Knowledge of organizational privacy governance models, including centralized and decentralized privacy structures
8. Ability to identify the roles and responsibilities of privacy professionals and cross-functional teams involved in privacy compliance	8. Knowledge of privacy compliance roles and cross-functional teams including legal, technical, and hybrid governance functions
9. Ability to identify the skills and competencies required for effective data privacy officer performance	9. Knowledge of professional skills and competencies required for effective data privacy officer functions

Domain 3: Consumer rights, business obligations, and compliance

Main objective: Ensure that the candidate is able to interpret and operationalize consumer privacy rights, organizational compliance obligations, and regulatory requirements related to personal data processing, consumer requests, and vendor or cross-border data management.

Competencies	Knowledge statements
1. Ability to interpret consumer privacy rights and corresponding business obligations under major U.S. privacy regulations 2. Ability to implement organizational processes for providing required privacy notices and disclosures to consumers 3. Ability to manage and operationalize consumer rights request processes within an organization 4. Ability to implement procedures for handling specific consumer rights requests including access, deletion, correction, and opt-out requests 5. Ability to implement identity verification processes and procedures when responding to consumer privacy requests 6. Ability to apply regulatory requirements for protecting the privacy rights of minors 7. Ability to evaluate common consumer rights and shared compliance obligations across multiple U.S. state privacy laws 8. Ability to identify state-specific consumer rights and organizational compliance requirements under U.S. state privacy laws 9. Ability to manage privacy compliance requirements related to vendors and third-party service providers 10. Ability to assess regulatory considerations and compliance requirements for data transfers across U.S. states and international jurisdictions 11. Ability to evaluate frameworks and mechanisms supporting cross-border data transfers	1. Knowledge of consumer rights and business obligations established under the California Consumer Privacy Act (CCPA) and related regulations 2. Knowledge of regulatory requirements governing the collection, use, and disclosure of personal information 3. Knowledge of required privacy notices and disclosures, including privacy policies, notice at collection, opt-out notices, and notices related to sensitive personal information 4. Knowledge of procedures for managing consumer privacy requests, including intake mechanisms, accessibility considerations, acknowledgment requirements, and response timelines 5. Knowledge of processes for handling deletion, correction, disclosure, and opt-out of sale or sharing requests 6. Knowledge of mechanisms for limiting the use of sensitive personal information and managing opt-in requests after opt-out actions 7. Knowledge of identity verification requirements and verification methods for both account holders and non-account holders, including requests submitted by authorized agents 8. Knowledge of privacy protections and regulatory requirements applicable to minors 9. Knowledge of shared consumer rights and controller or business compliance obligations across U.S. state privacy laws 10. Knowledge of state-specific consumer rights and business compliance requirements across U.S. privacy regulations 11. Knowledge of vendor management requirements and contractual obligations under the CCPA 12. Knowledge of regulatory considerations and compliance steps for data transfers across the U.S.

Competencies	Knowledge statements
	13. Knowledge of regulatory considerations and compliance mechanisms for cross-border data transfers, including the Data Privacy Framework and related transfer safeguards

Domain 4: Privacy management and data security measures

Main objective: Ensure that the candidate is able to evaluate privacy risks, implement appropriate data protection measures, and oversee technical and organizational safeguards designed to protect personal information.

Competencies	Knowledge statements
1. Ability to explain the objectives and components of a privacy risk assessment process 2. Ability to identify stakeholders and organizational roles involved in privacy risk assessments 3. Ability to apply risk assessment methodologies and analytical approaches to evaluate privacy risks 4. Ability to interpret privacy risk assessment requirements within U.S. federal and state regulatory frameworks 5. Ability to apply recognized risk assessment frameworks and methodologies used in privacy and security governance 6. Ability to evaluate the role of data security measures in protecting personal information and supporting privacy compliance 7. Ability to identify and implement appropriate access control and identity management safeguards for protecting personal data 8. Ability to assess network security controls and monitoring technologies used to prevent unauthorized access and data compromise 9. Ability to evaluate data protection technologies designed to prevent unauthorized disclosure or loss of personal information 10. Ability to manage information and asset inventories related to personal data and supporting information systems 11. Ability to evaluate endpoint, application, and system security safeguards designed to protect personal data 12. Ability to recognize ethical considerations associated with protecting personal data and implementing security controls	1. Knowledge of the privacy risk assessment process and its role in identifying and mitigating risks to personal information 2. Knowledge of organizational stakeholders involved in risk assessments and their respective responsibilities 3. Knowledge of risk assessment methodologies and analytical approaches used in privacy risk analysis 4. Knowledge of privacy risk assessment requirements within U.S. federal privacy laws and state-level privacy regulations 5. Knowledge of the NIST risk assessment process and related governance frameworks 6. Knowledge of the importance of data security measures for protecting personal information and maintaining privacy compliance 7. Knowledge of key access control mechanisms including account management, separation of duties, least privilege, session control, remote access security, and mobile device access controls 8. Knowledge of network security safeguards including network segmentation, monitoring mechanisms, intrusion detection and prevention technologies, and bot detection technologies 9. Knowledge of data protection technologies such as data loss prevention solutions, vulnerability scanning, penetration testing, and masking of sensitive personal information 10. Knowledge of information and asset inventory management practices including data mapping, data flow documentation, classification, tagging mechanisms, and hardware and software inventory management 11. Knowledge of physical security measures for protecting personal information including facility access controls, secure storage, and clean-desk policies

Competencies	Knowledge statements
	12. Knowledge of endpoint and application security safeguards including secure development practices, code review, security testing, port and protocol control, and antivirus or anti-malware protections 13. Knowledge of ethical considerations related to protecting personal data and implementing data security controls

Domain 5: Records management and privacy audit

Main objective: Ensure that the candidate is able to implement documentation and record-keeping practices, maintain regulatory processing records, and evaluate privacy and cybersecurity compliance through structured audit processes.

Competencies	Knowledge statements
1. Ability to explain the role of documentation and record-keeping in privacy governance and regulatory compliance 2. Ability to identify regulatory documentation and record-keeping requirements under U.S. privacy laws and regulations 3. Ability to implement organizational practices for managing records related to personal data processing 4. Ability to manage documentation life cycle processes including record creation, retention, storage, and secure disposal 5. Ability to explain the objectives and functions of privacy and cybersecurity audits 6. Ability to distinguish between different types of audits 7. Ability to apply audit principles and methodologies in evaluating privacy and cybersecurity compliance 8. Ability to evaluate regulatory cybersecurity audit requirements and internal audit activities supporting privacy governance	1. Knowledge of documentation and record-keeping practices supporting privacy governance and regulatory accountability 2. Knowledge of documentation requirements established by the Federal Trade Commission for privacy and data security compliance 3. Knowledge of documentation requirements established under the rule issued pursuant to Executive Order 14117 4. Knowledge of documentation and record-keeping requirements across U.S. state privacy laws 5. Knowledge of documentation life cycle management including record creation, maintenance, retention schedules, and secure disposal 6. Knowledge of the purpose, scope, objectives, and types of cybersecurity and privacy audits 7. Knowledge of core audit principles including independence, objectivity, evidence collection, and audit reporting 8. Knowledge of cybersecurity audit requirements under the GLBA 9. Knowledge of cybersecurity audit requirements established under the Final Rule issued pursuant to Executive Order 14117 10. Knowledge of cybersecurity audit requirements established under CCPA regulations 11. Knowledge of internal audit services and activities supporting cybersecurity and privacy compliance programs

Domain 6: Incident management, monitoring, and continual improvement

Main objective: Ensure that the candidate is able to manage privacy and data security incidents, coordinate response activities, implement breach notification requirements, and support continuous improvement through monitoring and training programs.

Competencies	Knowledge statements
1. Ability to explain the nature and implications of personal information security breaches within organizational and regulatory contexts 2. Ability to establish and coordinate incident management processes for responding to privacy and data security incidents 3. Ability to identify organizational roles and responsibilities involved in incident response and breach management 4. Ability to implement structured incident response activities including containment, eradication, and recovery 5. Ability to evaluate regulatory obligations related to incident reporting and breach notification 6. Ability to design and promote privacy and security awareness training programs within organizations 7. Ability to implement monitoring and review mechanisms to assess privacy and data protection practices 8. Ability to support continuous improvement of privacy and security programs through monitoring, training, and governance activities	1. Knowledge of personal information security breaches and their impact on privacy governance and regulatory compliance 2. Knowledge of incident management principles and processes for responding to privacy and data security incidents 3. Knowledge of the NIST incident management framework and incident response life cycle 4. Knowledge of incident response requirements under the Code of Federal Regulations (CFR) 5. Knowledge of FTC guidance related to data breach response and incident handling 6. Knowledge of roles and responsibilities of incident response teams involved in privacy and data security incidents 7. Knowledge of incident response activities including containment, eradication, and recovery processes 8. Knowledge of breach notification requirements, notification content, and reporting procedures 9. Knowledge of the importance and objectives of employee privacy and security training programs 10. Knowledge of key components of effective privacy awareness and training initiatives 11. Knowledge of training requirements established under U.S. privacy regulations including the CCPA 12. Knowledge of monitoring and review mechanisms supporting privacy compliance and risk management 13. Knowledge of continuous security monitoring principles and monitoring tools used to detect and manage privacy and security risks

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	Privacy foundations and regulatory framework	20	25%	X	
	Privacy governance, leadership, and organizational roles	7	8.75%		X
	Consumer rights, business obligations, and compliance	15	18.75%		X
	Privacy management and data security measures	20	25%	X	
	Records management and privacy audit	9	11.25%		X
	Incident management, monitoring, and continual improvement	9	11.25%		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%**.

This exam comprises multiple-choice questions: The multiple-choice exam can be used to evaluate candidates' understanding of 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-dependent, whereas scenario-based questions are context-dependent, i.e., they are developed based on a scenario that 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 U.S. privacy and data protection regulations referenced in the training course
- 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 sample of exam questions will be provided below.

Sample Exam Questions

MeryAnalytics is a U.S.-based technology company that provides cloud-based data analytics platforms for healthcare providers and insurance companies. Because the company processes large volumes of personal and medical data, *MeryAnalytics* has appointed a data privacy officer (DPO) responsible for ensuring compliance with privacy regulations and overseeing the protection of personal information across the company's systems.

As part of *MeryAnalytics*'s annual security and privacy program review, the DPO instructed the cybersecurity team to analyze the company's infrastructure for weaknesses that could expose sensitive patient data. The team deployed automated scanning tools across *MeryAnalytics*'s network infrastructure, servers, and databases. The scans generated a report identifying potential weaknesses such as open ports, outdated software versions, and misconfigured services.

After reviewing the findings, the DPO approved a deeper security evaluation to determine whether these weaknesses could actually be exploited. *MeryAnalytics* hired external cybersecurity consultants who conducted a structured test. During the test, the consultants first defined the objectives and obtained management approval. Next, they initiated testing and analyzed vulnerabilities using internal and public vulnerability databases. Then, they attempted to exploit the identified weaknesses by gaining access to systems, escalating privileges, and navigating the network. Finally, the consultants produced a report summarizing the vulnerabilities and recommending mitigation actions.

At the same time, the DPO led a review of *MeryAnalytics*'s internal analytics platform used by customer support analysts. The review revealed that analysts with limited privileges could view full patient identification numbers and insurance details. To reduce unnecessary exposure of sensitive information, the engineering team implemented a control that hides sensitive fields depending on the user's role while keeping the original data unchanged in the system.

MeryAnalytics also improved the protection of customer data stored in its cloud environment. The company implemented an encryption method that ensures sensitive information such as phone numbers and account identifiers remain in the same format and length after encryption so that existing applications can continue to process the data without modification.

Finally, the DPO reviewed how secure communications were implemented across *MeryAnalytics*'s systems. The company confirmed that a specific protocol is used to provide secure remote administrative access to internal servers. Because this protocol is designed for remote system administration rather than protecting web communications, the DPO decided it should not be used for securing customer-facing web transactions.

1. Which type of tool did *MeryAnalytics* use to scan its servers and workstations for vulnerabilities?
 - A. Network-based scanning tool
 - B. **Host-based scanning tool**
 - C. Wireless network scanning tool

2. Did *MeryAnalytics* conduct the stages of this security exercise appropriately according to the penetration testing process defined in NIST SP 800-115?
 - A. **Yes, the four stages were conducted appropriately according to NIST SP 800-115.**
 - B. No, as testers should not use internal or public vulnerability databases.
 - C. No, as the objectives should not be defined during the planning stage.

3. Which masking technique did *MeryAnalytics*'s engineering team implement?
 - A. Static data masking
 - B. **Dynamic data masking**
 - C. On-the-fly masking

4. Which encryption technique was implemented by *MeryAnalytics* to protect its customer data?
 - A. **Format-preserving encryption**
 - B. RSA encryption
 - C. AES encryption

5. Which protocol did the DPO decide to exclude from *MeryAnalytics*'s customer-facing web transaction systems?
 - A. TLS/SSL
 - B. IPsec
 - C. **SSH**

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB Certified U.S. Data Privacy Officer Credentials

All PECB certifications have specific requirements regarding 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 Certified U.S. Data Privacy Officer scheme have the following requirements:

Credential	Exam	Professional experience	MS project experience	Other requirements
PECB Certified Provisional U.S. Data Privacy Officer	PECB Certified U.S. Data Privacy Officer	None	None	Signing the PECB Code of Ethics
PECB Certified U.S. Data Privacy Officer		Five years: Two years of work experience in U.S. privacy laws and regulations	Project activities: a total of 300 hours	

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

1. Publishing and maintaining a compliant privacy policy describing data practices and consumer rights
2. Offering mechanisms for consumers to exercising rights to know, delete, correct, and opt out
3. Governing service providers, contractors, and third-party data disclosures through required contracts
4. Limiting collection, use, retention, and sharing of personal information to necessary and proportionate purposes
5. Conducting privacy risk assessments and overseeing automated decision-making technology
6. Maintaining a cybersecurity program and completing required cybersecurity audits
7. Delivering workforce privacy training and retaining compliance-related records

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking [here](#).

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

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

- [Create](#) your account
- Check your email for the confirmation link
- [Log in](#) and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If approved, you will then be able to download your certificate and digital badge from your member account.

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 CV.

Professional References

For each application, two professional references are required. Professional references shall be individuals who have worked with you in a professional environment and can validate your expertise in the respective field, current, and previous work history. You cannot use as a reference the persons who fall under your supervision or are a relative of yours.

Project Experience

The candidate's project log will be checked to ensure that the candidate has the required number of implementation 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.

PECB can deny certification/certificate program if candidates:

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

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process [Complaint and Appeal Policy](#).

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. 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.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking [here](#).

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 continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in [here](#), clicking **View Certificate**, and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the [Certification Maintenance](#) page on the PECB website.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been revoked are not authorized to use any references to a certified status.

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the [Certification Maintenance](#) page on the PECB website.

SECTION V: OTHER POLICIES

Application Fees for Examination and Certification

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

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is as follows:

- Master Certification: \$100
- Foundation Certification: \$200
- Transition Certification: \$200
- All other Certifications: \$500

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a [service ticket](#) and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the [complaint and appeal policy](#).

Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

PECB will refund your payment if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

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



Contact PECB Support at
support@pecb.com



Telephone number
+1-844-426-7322



Visit our [Help Center](#) to access manuals, FAQs, and quick guides, or reach us directly via Live Chat or by submitting a ticket [here](#).

Follow us on:



www.pecb.com