Version 2.0; Last update: July 20, 2026

1. Purpose

PECB is committed to protecting the Personal Data of its employees, clients, certification/certified candidates, trainees, trainers, auditors, invigilators, partners, distributors, contractors, suppliers, website users, and other individuals whose Personal Data it processes.

This Policy establishes the organization-wide principles, responsibilities, and governance requirements for the lawful, fair, transparent, secure, and accountable collection, use, disclosure, storage, transfer, retention, and disposal of Personal Data by or on behalf of PECB.

Its purpose is to ensure that Personal Data is processed lawfully, fairly, transparently, securely, and in accordance with applicable data protection and privacy laws.

2. Scope

This Policy applies to:

- All PECB employees, officers, managers, contractors, consultants, temporary workers, and other persons who process Personal Data for or on behalf of PECB;
- Personal Data in any form, including electronic, physical, verbal, visual, or recorded information;
- All PECB systems, services, applications, platforms, locations, remote-working environments, and approved third-party environments; and
- All third parties processing Personal Data on behalf of PECB.

This Policy applies regardless of where Personal Data is accessed, stored, transferred, or processed.

3. Applicable Data Protection Legislation

PECB shall comply with the Singapore Personal Data Protection Act 2012 (PDPA) and Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), including applicable regulatory guidance, whenever each framework applies to a Personal Data processing activity. The PDPA and GDPR shall be treated as equally applicable components of PECB's organization-wide data protection framework within their respective territorial and material scopes.

PECB shall also comply with other applicable data protection and privacy laws in the countries and jurisdictions in which it operates or provides services, together with relevant contractual, accreditation, and regulatory requirements.

Where more than one data protection law applies to the same processing activity, PECB shall identify and comply with the applicable requirements under each relevant legal framework. Where those requirements differ or overlap, PECB shall implement appropriate measures to fulfil the relevant applicable obligations and shall obtain advice from the Data Protection Officer or Legal Officer where necessary.

The identity of the relevant PECB controller, together with current external contact details for the Data Protection Officer and, where applicable, PECB's representative in the European Union, shall be publicly available.

4. Definitions

For this Policy, the following definitions apply:

Personal Data means any information relating to an identified or identifiable natural person, whether the information is accurate or not and whether recorded in material form or otherwise.

Processing means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure, transmission, restriction, deletion, anonymization, or destruction.

Data Subject means the individual to whom Personal Data relates.

Controller means an organization that determines the purposes and means of processing Personal Data.

Processor means an organization that processes Personal Data on behalf of a controller.

Data Intermediary means an organization that processes Personal Data on behalf of and for the purposes of another organization, as understood under the Singapore PDPA.

Consent means a freely given, specific, informed, and unambiguous indication of an individual's agreement to the processing of Personal Data, where this standard is required by applicable law.

Special Category Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for unique identification, health information, or information concerning a person's sex life or sexual orientation.

Sensitive Personal Data means Personal Data that may create a higher risk to the individual if improperly accessed, used, or disclosed, including identification documents, financial information, account credentials, examination records, sanctions-screening results, and Special Category Data.

Personal Data Breach means a security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Anonymization means the processing of Personal Data so that the information can no longer be associated with an identifiable individual by reasonably available means.

Pseudonymization means processing Personal Data so that it cannot be attributed to a specific individual without the use of additional information kept separately and securely.

5. Data Protection Principles

PECB shall process Personal Data in accordance with the following principles:

Lawfulness, fairness, and transparency - Personal Data shall be processed lawfully, fairly, and in a manner that individuals can reasonably understand.

Purpose limitation - Personal Data shall be collected, used, and disclosed only for specified, explicit, legitimate, and reasonable purposes. It shall not be processed for an incompatible purpose unless permitted by applicable law.

Data minimization - Only Personal Data that is adequate, relevant, and reasonably necessary for the intended purpose shall be collected and processed.

Accuracy - Reasonable steps shall be taken to ensure that Personal Data is accurate, complete, and kept up to date where necessary.

Retention limitation - Personal Data shall not be retained for longer than necessary for the relevant business, contractual, legal, regulatory, accreditation, certification, complaint, appeal, security, or evidentiary purpose.

Integrity and confidentiality - Personal Data shall be protected through appropriate technical, physical, and organizational measures proportionate to the nature, sensitivity, and risks of the processing.

Accountability - PECB shall maintain appropriate policies, procedures, records, training, assessments, controls, and monitoring activities to demonstrate compliance with applicable data protection requirements.

6. Governance and Responsibilities

All PECB employees and contractors, share responsibility for handling and protecting Personal Data appropriately in accordance with their assigned roles and applicable PECB requirements.

Top Management shall:

- Approve significant policies;
- Provide appropriate resources for privacy and data protection compliance;
- Promote a culture of privacy, confidentiality, and accountability;
- Ensure that material privacy risks are considered in organizational decision-making;
- Support the independence of the Data Protection Officer; and
- Review material privacy risks, incidents, audit findings, and corrective actions.

The Data Protection Officer shall:

- Inform and advise PECB and its personnel regarding data protection obligations;
- Monitor compliance with applicable data protection laws, this Policy, and related procedures;
- Oversee the implementation of PECB's privacy governance framework;
- Advise on Data Protection Impact Assessments and privacy risk assessments;
- Support the handling of Data Subject requests;
- Support the assessment, management, and notification of Personal Data Breaches;
- Cooperate with competent supervisory and regulatory authorities;
- Act as a contact point for authorities and Data Subjects;
- Support privacy training and awareness activities;
- Monitor privacy-related corrective actions; and
- Report significant privacy matters to Top Management.

The Data Protection Officer shall be involved in a timely manner in matters involving material Personal Data processing and shall perform the role with appropriate independence, resources, confidentiality, and access to Top Management.

Information Security Operations Specialist shall:

- Implement and maintain appropriate security controls;
- Conduct information-security risk assessments;
- Manage identity, access, authentication, encryption, monitoring, and endpoint-security controls;
- Support vulnerability management and security testing;
- Support the investigation, containment, and remediation of Personal Data Breaches;
- Maintain security incident records; and
- Report material security risks to the Data Protection Officer and Top Management.

Managers and Process/Module Owners shall:

- Identify the Personal Data processed and the purpose for processing it;
- Ensure that privacy notices and consent mechanisms are implemented where required;
- Restrict access to persons with an authorized business need;
- Define access requirements;
- Approve and periodically review user access;
- Update and Apply approved retention and disposal requirements;
- Notify the Data Protection Officer before introducing or materially changing processing activities;
- Ensure that identified privacy risks and corrective actions are addressed.
- Support secure deletion, anonymization, export, and correction of Personal Data.

Contract Owners responsible for third-party relationships shall:

- Conduct appropriate privacy and security due diligence;
- Ensure that required contractual data protection clauses are implemented;
- Consult the Data Protection Officer before engaging processors or service providers involving material Personal Data;
- Ensure that Personal Data is returned, transferred, or securely deleted when a service relationship ends.

Employees and contractors shall:

- Process Personal Data only for authorized business purposes;
- Follow this Policy and related procedures;
- Maintain confidentiality;
- Use only approved systems and communication channels;
- Protect credentials and access rights;
- Complete required privacy and security training;
- Immediately report suspected Personal Data Breaches, unauthorized disclosures, or policy violations; and
- Cooperate with privacy investigations, audits, and corrective actions.

7. Legal Grounds, Consent, and Permitted Processing

Before processing Personal Data, PECB shall identify and document the legal permission applicable to the processing activity under the relevant law.

Singapore PDPA

Where the Singapore PDPA applies, PECB shall collect, use, or disclose Personal Data only:

- With the individual's consent;
- Where consent is deemed under applicable law;
- Where a permitted exception to consent applies; or
- Where otherwise authorized or required by law.

EU GDPR

Where the GDPR applies, PECB shall identify an appropriate lawful basis, which may include:

- The Data Subject's consent;
- Performance of a contract or pre-contractual steps requested by the Data Subject;
- Compliance with a legal obligation;
- Protection of vital interests;
- Performance of a task carried out in the public interest, where applicable; or
- PECB's legitimate interests or the legitimate interests of a third party, provided that those interests are not overridden by the rights and freedoms of the Data Subject.

Consent Management

Where consent is required, PECB shall ensure that consent is:

- Obtained before the relevant processing begins;
- Provided through clear and understandable language;
- Specific to the relevant purpose;
- Separate from unrelated terms where appropriate;
- Capable of being withdrawn; and
- Modified where the purpose or nature of processing materially changes.

Withdrawal of consent shall not affect processing already lawfully carried out before withdrawal.

PECB may continue processing where another lawful basis, legal obligation, contractual requirement, accreditation requirement, or permitted exception applies.

8. Collection, Transparency and Privacy Statement

PECB shall provide individuals with clear and accessible information about how their Personal Data is processed.

Privacy Statement shall include, where applicable:

- The identity and contact details of the relevant PECB entity;
- The purposes for which Personal Data is processed;
- The applicable lawful basis or legal permission;
- The categories of Personal Data processed;
- Information concerning processors and third-party service providers;
- International transfers and applicable safeguards;
- Retention periods;
- Data Subject rights and complaint options;

Where Personal Data is collected directly from the individual, the relevant statement shall be provided at or before collection.

9. Data Handling Requirements

9.1. Data Minimization and Accuracy

- PECB shall limit the collection and processing of Personal Data to what is reasonably necessary for the relevant purpose.
- PECB shall periodically review forms, platform fields, databases, employee records, examination and certification records, marketing records, audit records, and other repositories containing Personal Data.
- Information/records that are unnecessary, excessive, duplicated, or no longer relevant shall be removed, anonymized, or discontinued where appropriate.
- PECB shall provide reasonable mechanisms for individuals to review, update, or correct their Personal Data.

9.2. Special Category and Sensitive Personal Data

PECB shall process Special Category Data, criminal background records, health information, identification documents, financial information, and other Sensitive Personal Data only where:

- The processing is necessary for a defined purpose;
- An appropriate legal basis and any required additional condition have been identified;
- Collection is proportionate to the purpose;
- Access is limited to specifically authorized personnel;
- Enhanced safeguards are applied;
- Retention is limited; and
- Privacy risks are assessed where appropriate

Sensitive Personal Data shall not be collected merely because it may be useful in the future.

9.3. Children's Personal Data

PECB's websites and services are not intended for children (persons under the age of 16), and PECB does not knowingly collect their Personal Data.

Where PECB becomes aware that Personal Data has been collected from a child without the required authorization, reasonable steps shall be taken to restrict, correct, or delete the information in accordance with applicable law.

10. Privacy by Design, Records, and Risk Assessments

Privacy requirements shall be considered when designing, acquiring, developing, implementing, or materially changing systems, services, products, business processes, artificial-intelligence tools, monitoring or screening activities, marketing activities, employee processes, and third-party arrangements.

By default, PECB shall:

- Collect only necessary Personal Data;
- Limit access according to role and business need;
- Use privacy-protective settings;
- Limit retention;
- Prevent unrestricted availability of Personal Data; and

- Apply appropriate security controls.

10.1. Personal Data Inventory and Records of Processing

PECB shall maintain Records of Processing Activities (RoPA) containing:

- The activity and responsible Process Owner;
- Categories of Data Subjects and Personal Data;
- Processing purposes and lawful basis or legal permission;
- Systems and locations used;
- Recipients and processors;
- International transfers;
- Retention periods;
- Security measures;
- Relevant privacy statements;
- Automated processing.

Process Owners shall notify the Data Protection Officer when a processing activity is created, materially changed, transferred, outsourced, or discontinued.

10.2. Privacy Risk Assessments and DPIAs

A privacy risk assessment shall be completed before processing begins or materially changes where the activity may create significant risk to individuals.

Where the GDPR applies, a Data Protection Impact Assessment shall be completed when processing is likely to result in high risk to individuals' rights and freedoms.

Assessment may be required for:

- Systematic or large-scale monitoring;
- Special Category Data or biometric identification;
- Artificial intelligence, profiling, or automated decision-making;
- Processing involving vulnerable individuals;
- Large-scale processing; or
- New or emerging technologies.

11. Automated Processing, Screening, and Profiling

Where PECB uses automated processing, screening, monitoring, or profiling, it shall:

- Define and document the purpose;
- Identify the applicable legal basis, consent/permission;
- Inform affected individuals where required;
- Assess the quality, relevance, and accuracy of the information used;
- Implement safeguards against incorrect, unfair, or discriminatory outcomes;
- Restrict access to results;
- Establish appropriate retention periods;
- Provide human review where required or appropriate; and
- Enable individuals to question or challenge decisions where applicable.

For sanctions-list screening, PECB shall ensure that potential matches are reviewed before adverse action is taken, false positives are managed, access is restricted, and results are retained only as necessary.

PECB shall not make decisions based solely on automated processing that produce legal or similarly significant effects unless permitted by applicable law and supported by appropriate safeguards.

12. Data Subject Rights and Request Handling

Individuals may exercise the rights available under applicable law. Depending on the jurisdiction, these may include the right to:

- Receive information about processing;
- Access Personal Data and obtain a copy;
- Correct inaccurate or incomplete Personal Data;
- Request erasure or restriction;
- Object to processing;
- Receive Personal Data in a readable format;
- Withdraw consent;
- Obtain safeguards concerning certain solely automated decisions;
- Request human review of certain automated decisions; and
- Lodge a complaint with a competent authority.

These rights are not absolute and may be limited by applicable legal conditions, exemptions, retention duties, accreditation or certification requirements, legal claims, or the rights of others.

12.1. Submitting a Request, Question or Complaint

Routine requests to correct or modify private data may be submitted to PECB Customer Support at support@pecb.com or through the **Submit a Ticket** option in the PECB Help Center.

Other requests, suggestions, or complaints concerning the processing of your Personal Data, should be addressed to the Data Protection Officer at dpo@pecb.com.

In accordance with Article 27 of the GDPR, PECB has appointed a representative in the European Union, located in Lisbon, Portugal. The representative may be contacted at gdpr.representative@pecb.com.

12.2. Verification, Fees, and Timing

Individuals may exercise the rights available under applicable law.

PECB shall:

- Use reasonable and proportionate measures to verify the requester's identity and authority;
- Avoid requesting more Personal Data than necessary for verification;
- Handle requests free of charge unless a fee is permitted by law (*a fee is applicable for multiple DSAR requests*) ;
- Notify the requester in advance if a lawful fee applies;
- Respond without undue delay and within the applicable legal timeframe; and
- Inform the requester within the initial response period if a lawful extension is required.

12.3. Refusal, Limitation, and Erasure

Where a request is refused or limited, PECB shall explain the reasons, subject to legal restrictions, and identify available complaint or appeal options.

PECB may retain information requested for erasure where necessary for:

- Legal or regulatory compliance;
- Certification or accreditation obligations;
- Contractual obligations;
- Complaint and appeal handling;
- Fraud prevention;
- Legal claims;
- Security, audit, financial, or accounting records; or
- Another lawful and documented purpose.

Before deleting an account or related records, PECB shall explain relevant consequences, including possible loss of access to certification records, examination records, training materials, or services.

13. Marketing and Service Communications

Where required, PECB shall obtain consent before sending marketing communications about training courses, newsletters, webinars, events, promotions, or related services.

Recipients shall be able to withdraw consent or unsubscribe easily.

PECB may use contact details obtained through an existing client relationship to send targeted relevant communications, including communications with a promotional element, about PECB's own services that are similar or closely related to that relationship and reasonably considered relevant or important. Such communications may be sent based on PECB's legitimate interests or an applicable existing-customer exception, and recipients may object or unsubscribe at any time.

PECB may send non-promotional service communications necessary to:

- Create or manage accounts;
- Administer certifications, training, examinations, applications, payments, or invoices;
- Provide customer support;
- Communicate security, legal, regulatory, accreditation, policy, or contractual matters; or
- Notify users of changes affecting active services.

Recipients generally cannot opt out of necessary service communications while the relevant account, registration, certification, examination, contract, or service remains active. Service communications shall not include unnecessary promotional content.

Independent PECB partners may process Personal Data and send communications under their own privacy statements. PECB is not responsible for a partner's independent marketing activities.

14. Retention and Secure Disposal

Personal Data shall be retained according to PECB's approved retention schedule.

Retention periods shall consider:

- The original processing purpose;
- Contractual obligations;
- Certification, accreditation, examination, and training requirements;
- Legal, regulatory, financial, and accounting obligations;
- Complaint, appeal, limitation, audit, and investigation periods;
- Fraud-prevention requirements; and
- Legitimate evidentiary needs.

PECB shall review retained Personal Data periodically.

When information is no longer required, it shall be securely deleted, destroyed, irreversibly anonymized, or otherwise disposed of using an approved method.

Hard-copy records shall be securely shredded or destroyed by an approved confidential-destruction service. Electronic records shall be deleted using approved methods appropriate to the system and storage medium.

Where immediate deletion from backups is not technically feasible, access shall be restricted and the information shall not be restored or used except for legitimate recovery purposes.

Deletion may be suspended where information is subject to a legal hold, investigation, complaint, appeal, audit, regulatory or accreditation requirement, or actual or anticipated legal claim.

15. Data Security and Working Practices

PECB shall implement technical, physical, and organizational measures proportionate to the nature, volume, sensitivity, context, and risk of the Personal Data processed.

Controls may include:

- Information classification, least privilege, need-to-know access, and segregation of duties;
- Strong authentication, multi-factor authentication, and periodic access reviews;
- Encryption in transit and at rest where appropriate;
- Secure communication protocols, logging, monitoring, and data-loss prevention;
- Endpoint, firewall, network, vulnerability, and patch-management controls;
- Secure backup, recovery, business continuity, and disaster-recovery controls;
- Physical access controls and clean-desk practices;
- Secure software-development practices, penetration testing, and security assessments; and
- Approved retention and secure-disposal mechanisms.

15.1. Electronic and Physical Records

Electronic Personal Data shall be stored and transmitted only through approved systems, devices, cloud services, and secure methods. Unnecessary local copies shall not be kept on personal or unapproved devices.

Physical records shall be stored in locked or otherwise secure areas, accessed only by authorized personnel, protected during transport, and securely destroyed when no longer required.

15.2. Removable Media

Personal Data shall not be stored on removable media without documented business need and authorization. Approved removable media shall be encrypted where feasible, physically secured, tracked where appropriate, and securely erased or destroyed after use.

15.3. Personnel Practices

Personnel shall:

- Lock screens when devices are unattended;
- Protect passwords and authentication credentials;
- Verify recipients before transmitting Personal Data;
- Avoid unapproved communication or storage channels;
- Use only authorized applications and storage locations;
- Prevent unauthorized viewing or overhearing; and
- Report suspicious activity immediately.

16. Processors, Service Providers, and Partners

Before appointing a processor, data intermediary, cloud provider, software provider, or other service provider that will process Personal Data, PECB shall conduct proportionate privacy and security due diligence.

Due diligence shall consider:

- The nature, sensitivity, purpose, and volume of processing;
- Processing and storage locations;
- Security controls and breach history;
- Support for Data Subject requests; and
- International-transfer arrangements.

Written agreements shall address, where applicable:

- Processing subject matter, duration, nature, and purpose;
- Documented instructions and confidentiality;
- Security requirements;
- Assistance with Data Subject requests and breach response;
- Audit and assurance rights;
- International transfers;
- Return or deletion of Personal Data; and
- Obligations upon termination.

Processors and data intermediaries processes data according to their own privacy policies.

Where PECB acts as a processor or data intermediary, it shall follow the relevant contract, documented instructions, and applicable law.

Independent partners are responsible for processing activities for which they determine the purposes and means. Where PECB and another organization jointly determine those purposes and essential means, their responsibilities shall be documented in an appropriate arrangement.

17. International Data Transfers

Personal Data shall be transferred outside Singapore, the EEA, or another originating jurisdiction only in accordance with applicable law.

For transfers from Singapore, PECB shall take appropriate steps to ensure that the overseas recipient provides a standard of protection comparable to that required by the Singapore PDPA and GDPR.

Permitted safeguards may include:

- Contractual obligations;
- Binding corporate rules or internal group arrangements;
- Legally recognized certifications;
- Statutory exemptions;
- Other legally permitted mechanisms.
- An adequacy decision;
- Standard Contractual Clauses;

18. Disclosure of Personal Data

PECB may disclose Personal Data only:

- For an authorized and documented purpose;
- With valid consent where required;
- To an approved processor, service provider, or authorized PECB partner;
- To accreditation or certification bodies where necessary;
- To competent authorities;
- Where required by law, court order, or legal process;
- For the establishment, exercise, or defense of legal claims;
- To protect the rights, property, safety, or security of PECB or others; or
- Where another applicable legal permission exists.

Requests from courts, regulators, law enforcement agencies, or public authorities shall be reviewed for lawfulness, scope, and authenticity. Legal advice shall be obtained where appropriate.

Only the minimum Personal Data legally or reasonably necessary shall be disclosed.

19. Personal Data Breach Management

All suspected or confirmed Personal Data Breaches shall be reported immediately through PECB's incident-reporting process. Personnel shall not delay reporting while attempting to investigate independently.

PECB shall:

- Contain the incident and preserve relevant evidence;
- Identify affected systems, records, data categories, approximate volume, and individuals;
- Assess the cause, impact, likelihood, and severity of harm;
- Determine applicable notification requirements and deadlines;
- Notify competent authorities and affected individuals where required;
- Document the assessment, decisions, and notifications;

- Implement corrective and preventive actions; and
- Review the effectiveness of the response.

All breaches shall be recorded, including those that do not require external notification.

Where the Singapore PDPA applies, PECB shall assess whether notification to the Personal Data Protection Commission and affected individuals is required within the prescribed timeframes.

Where the GDPR applies, PECB shall assess whether notification to the competent supervisory authority and communication to affected Data Subjects are required.

Processors, data intermediaries, service providers, and partners shall be contractually required to notify PECB of relevant breaches without undue delay.

Employees and contractors shall not independently notify affected individuals, authorities, clients, partners, or the media unless authorized. The DPO shall be responsible to manage and communicate with relevant stakeholders about the relevant breach

19.1. Training, Monitoring, and Compliance

Personnel with access to Personal Data shall receive appropriate privacy and information-security training:

- Upon joining PECB;
- Periodically thereafter;
- When responsibilities materially change; and
- Following significant legal, policy, system, or risk changes.

Role-specific training shall be provided where appropriate to personnel involved in Data Subject requests, marketing, human resources, information technology, information security, examinations, certification, partner management, incident response, or high-risk processing.

PECB shall assess compliance through proportionate:

- Privacy and risk reviews;
- Internal audits;
- Security testing;
- Corrective-action monitoring.

Nonconformities, weaknesses, and violations shall be documented and addressed. Material issues shall be reported to the Data Protection Officer and Top Management.

Failure to comply may result in disciplinary action, access restriction, contractual remedies, termination of employment or engagement, legal action, or regulatory reporting where required.

20. Policy Exceptions

An exception to this Policy may be approved only where:

- A documented business, legal, regulatory, or technical need exists;
- Privacy and security risks have been assessed;
- Appropriate alternative safeguards are implemented;

- The Data Protection Officer approves the exception;
- The exception is limited in scope and duration; and
- The exception is reviewed periodically.

No exception may authorize unlawful processing.

21. Policy Review

This Policy shall be reviewed at least annually and when there is:

- A significant change in applicable law;
- A significant change in PECB's structure, operating locations, systems, services, or processing activities;
- A significant Personal Data Breach;
- A regulatory, accreditation, or audit finding;
- A significant change in privacy risk or organizational responsibilities.

The Data Protection Officer shall coordinate the review.

22. Contact and Reporting

Questions, concerns, Data Subject requests, suspected Personal Data Breaches, or potential Policy violations shall be reported to:

Data Protection Officer
Email: dpo@pecb.com

Information Security Operations Specialist
Email: information.security@pecb.com

PECB Customer Service Help Center
Email: support@pecb.com

EEA Data Subjects may also contact the EEA Representative located in Lisbon, Portugal.

EEA Representative
Email: gdpr.representative@pecb.com