

Data Protection Policy

Introduction

Our Data Protection policy indicates that we are dedicated to and responsible for processing the information of our, customers, stakeholders, employees and other interested parties with absolute caution and confidentiality. This policy describes how we collect, store, handle and secure our data fairly, transparently, and with confidentiality.

This policy ensures that PECB follows good practices to protect the data gathered from its customers, employees, and stakeholders. The rules outlined in this document apply regardless of whether the data is stored electronically, on paper or on any other storage device.

1. Policy Elements

As a key part of our operations, we gather and process any information or data that makes an individual identifiable such as full name, physical address, email address, photographs, etc.

This information is collected only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply to our company.

Our data will:

- Be precise and consistently updated;
- Is collected legitimately and with a clearly stated purpose;
- Be processed by the company in line with its legal and ethical binds;
- Have protection measure that protects it from any unauthorized or illegal access occurring by internal or external parties.

Our data will NOT:

- Be communicated informally;
- Exceed the specified amount of time stored;
 - Therefore, personal data of employees, customers, and affiliates who no longer use PECB services will be archived for 3 years and deleted afterwards;
- Be transferred to organizations, states or countries that do not acquire proper data protection policies;
- Be spread to any party unless approved by the data's owner (except for the legitimate requests demanded from law enforcement authorities).

2. Roles and Responsibilities

Everyone who works for or with PECB is responsible for ensuring that the collection, storage, handling, and protection of data is being done appropriately. The contact person responsible for managing the Data Protection process is:

Person: **Information Security Manager**
Email: information.security@pecb.com
Phone: +1-844-426-7322

In addition, the following functions within PECB hold the key areas of responsibility:

Information Security Manager and Data Protection Officer (DPO) is responsible for:

- Informing and advising PECB in regards to the data protection and privacy for the natural persons;
- Monitoring Data Protection and privacy compliance of PECB with the data protection requirements applicable in Canada and EU;
- Providing advice with regard to data protection impact assessments;
- Cooperating and liaise with the supervisory authority;
- Be a point of contact for data subjects at: information.security@pecb.com;
- Providing oversight and continuous enhancement of cyber security and in risk management awareness programs and improvements;
- Collaborating with the Security Committee and leading the design, implementation, operation and maintenance of the Information Security Management System based on the ISO/IEC 27000 series standards;
- Ensuring periodic testing is conducted to evaluate the security posture of the Information Security by conducting periodic reviews of the ISMS to ensure compliance with the System Security Plans (SSP);
- Leading the design and operation of related compliance monitoring and improvement activities to ensure compliance with both internal security policies, and applicable laws and regulations;
- Developing and managing controls to ensure compliance with the wide variety and ever-changing requirements resulting from standards and regulations.

IT Systems Manager:

- Strictly complying with all PECB policies related to non-disclosure, non-competition and confidentiality of information;
- Constantly staying up to date on various web technologies and tools;
- Performing networking systems hardware and software upgrades, and installing security patches as needed;
- Checking and monitoring the general health of networks and networking devices;
- Performing daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled tasks;
- The implementation, configuration and maintenance of computer networks, software, and digital security.

Compliance Department:

- Ensuring data of the Certification holders, Certified Trainers, Auditors, Examiners, Examinees, and Invigilators is only accessible by authorized personnel;
- Ensuring that access to Certification holders, Trainers, Auditors, Examiners, Examinees, and Invigilators personnel data will not be shared with or provided to unauthorized personnel;
- Ensuring the additional documents and data provided by applicants is being stored appropriately and centralized to ensure the confidentiality, availability, and integrity of data.

Commercial Department:

- Ensuring that access to PECB Authorized Resellers and Distributors data is restricted for access only to authorized personnel;

- Ensuring that the access to PECB Authorized Resellers and Distributors data will not be shared with or provided to unauthorized personnel;
- Ensuring that access to the official PECB contact list data will not be shared with or provided to unauthorized personnel.

Systems Administrator:

- Ensuring that access to personal data of users registered on the PECB Website is restricted only to authorized personnel;
- Ensuring that access to the personal data of users registered on the PECB website will not be shared with or provided to unauthorized personnel.

3. General guidelines

- Access to data covered by this policy is restricted only to those who need it for their work;
- Data is not to be shared informally. When access to confidential information is required, employees request it from their line managers;
- We provide comprehensive training to all employees to help them understand their responsibilities when handling data;
- Employees keep all data secure, by taking sensible precautions and following the Data Storage guidelines specified below;
- In particular, strong passwords are used and never shared;
- Personal data is not disclosed to unauthorized people, within the company or externally;
- Employees request help from their line manager or the data protection officer when they are unsure about any aspect of data protection.

4. Data Storage

These rules describe how and where data are safely stored. When data is **stored on paper**, it is kept in a secure place accessed only by authorized personnel.

These guidelines also apply to data that is usually stored electronically but has been printed out for certain reasons:

- The paper or files are kept in a locked drawer or filing cabinet;
- Employees make sure paper and printouts are not left unattended;
- Data printouts are securely shredded and disposed when no longer needed.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious internal or external threats.

- Data should be protected by strong passwords that are updated regularly and never shared among employees;
- If data is stored on removable media (like a CD or DVD, External HDD, etc.), these should be kept locked away securely when not being used;
- PECB Network of computers is restricted from using or transferring any data via a CD, DVD, USB, and External HDD, unless authorized for specific personnel with additional privileges;
- Data should only be stored on designated servers at PECB premises, and should only be uploaded on to approved cloud computing services;

- Minimum requirements for encryption are AES 128 Bit. This is for data in transport or at rest. In premises and in the cloud;
- Secure communication is empowered with TLS (Transport Layer Security);
- Servers containing personal data are sited at secure locations, where access is restricted for authorized personnel only and monitored;
- Data is backed up daily. Backups are tested regularly, in line with the company's standard backup procedures;
- Data is never saved directly in permanent computers or other portable devices like tablets or smartphones, etc;
- All servers and computers containing data are protected by the monitoring system and the firewall system;
- All data entering into PECB systems and website are stored as associated with a specific user account to and measures to prevent privilege escalation are always in place;
- All data entering into the database of the PECB website are protected with certificates that ensure encrypted communication when receiving and sending information is being used.

5. Data usage

- All data collected by PECB is strictly for PECB-related services required to ensure a complete response/service is being provided by PECB. No other non-PECB related service will be offered from the data collected;
- When working with personal data, employees ensure their computer screens are always locked when left unattended;
- Data is encrypted before being transferred electronically;
- Employees do not save copies of personal data into their own computers. The access and update of a copy is always made at the central copy of the data.

6. Data accuracy and actions

To exercise data protection, PECB takes reasonable steps and is committed to:

- Restrict and monitor access to sensitive data, and keep it in as few places as possible;
- Establish effective data collection procedures;
- Provide employees with online privacy and security measures training;
- Build secure network to protect online data from cyber attacks;
- Establish clear procedures for reporting privacy breaches or data misuse;
- Include contract clauses or communicate statements on how we handle data;
- Update the data continuously and as mistakes are discovered;
- Ensure the marketing databases are checked against industry suppression files;
- Install tracking logs to monitor employee's activities ensuring data is not being misused;
- Install firewall and protection software that prevents employees to share and distribute data from PECB devices externally, by detecting when a large amount of data is being transferred either through email, or via external drives;
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.).

7. Subject access requests

All individuals and organizations who are the subject of personal and other data held by PECB are entitled to:

- Ask **what information** PECB holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request. Requests from individuals should be made by email, addressed to the data protection officer at information.security@pecb.com. The data controller can supply a standard request form, although individuals do not have to use this.

Our clients can contact us directly requesting these information through the subject access request. Such requests can be made via email addressed at our Data Protection Officer at information.security@pecb.com, or through the digital form available [here](#). We will always verify the identity of anyone making a subject access request before handing over any information. Confirmation will be asked from data subject using the email data subject used to register an account at PECB.

The first copy of a data subject will be provided free of charge by. However, a fee of 30\$ will be charged for further copies requested by the data subject. We will aim to provide the relevant data within 14 days.

7.1. Data Modification

Our clients can contact us requesting data modification and/or correction by sending an email to information.security@pecb.com or through the digital form available [here](#). PECB will verify the identity of anyone making a data subject access request before modifying or correcting any information.

7.2. Data erasure

Our clients can contact us requesting data erasure via email at information.security@pecb.com or through the digital form available [here](#). In addition, data subject will be provided with all necessary information before proceeding with erasure.

Before proceeding with the erasure, the data subject will read the statement of our data protection officer, explaining the outcome of the data being deleted. Erasure of data can be requested at any time.

8. Cross Border data transfer

Adequacy decisions by the European Commission in regards to cross border data transfer. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection. In addition, we ensure data protection and privacy for the information it possess for natural persons, therefore we are in compliance with the legislative requirements. The point of contact for all Data Protection Authorities (DPAs) and individuals in the EU on all issues related to data processing is **information.security@pecb.com**.

9. Children

Our website is not appealing to children, nor are they directed to children younger than 16. PECB does not knowingly collect personally identifiable data from persons under the age of 16, and strives to comply with the provisions of The Office of the Privacy Commissioner of Canada (OPC) and European Union



General Data Protection Regulation (EU GDPR). If you are a parent of a child under 16, and you believe that your child has provided us with information about him or herself, please contact us at **information.security@pecb.com**.

10. Disclosing Data

In certain circumstances, when required, PECB can disclose data to law enforcement agencies without the consent of the data subject. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

11. Privacy Policy

We have a privacy policy available on our website, stating out how data relating to customers, stakeholders, employees, and other parties involved is used in our company. Our data privacy policy is available here: <https://pecb.com/en/pecb-privacy-policy>