
Data protection concept of PEFC Switzerland

Copyright Notice

© PEFC Switzerland 2023

This document from PEFC Switzerland is freely available on request.

The document may not be reproduced or copied for commercial purposes without the permission of PEFC Switzerland.

Name of the document: Data protection concept of PEFC Switzerland

Title of the Document: SD 004

Adopted by: Board **Date:** 07.07.2023

Published on: 31.07.2023 **Entry into force on:** 31.07.2023

1. Purpose and scope	4
2. Legal basis	4
3. Terms	4
4. Scope	4
5. Objective	4
6. Principles of data protection	5
6.1. Legality	5
6.2. Proportionality	5
6.3. Earmarking	5
6.4. Transparency	5
6.5. Quality	5
6.6. Good faith	5
7. Data Security: Measures	6
7.1. Organizational measures	6
7.2. Technical measures	6
7.3. Archiving	6
7.4. Annihilation	6
8. Rights of data subjects	7
8.1. Enlightenment/Orientation	7
8.2. Right to information/inspection	7
8.3. Right to rectification	7
8.4. Blocking/refusal to disclose data	7
9. Instructions for action	8
9.1. How to behave in response to telephone and written enquiries	8
9.2. Principles of e-mail use	8
9.3. Use of image/sound recordings	8
10. Responsibilities	9
10.1. Board	9
10.2. Management	9
10.3. Employees	9

1. Purpose and scope

This data protection concept of PEFC Switzerland takes into account the importance and significance of data protection in terms of respecting the privacy and personal rights of its clients, its employees and, if necessary, its business partners. It forms the binding basis for all data protection-relevant measures and activities of PEFC Switzerland, in particular for the processing of

- personal data of the clients;
- personal data of employees, including data on job applications and former employees;
- Information about business partners and other third parties, as far as personal data is concerned.

2. Legal basis

The basis for this data protection concept is the Federal Data Protection Act of 25 September 2020 (DSG; SR 235.1) and the Data Protection Ordinance of 31 August 2022 (DPO; SR 235.11).

3. Terms

Important terms are defined in Appendix 1.

4. Scope

This data protection concept applies to all bodies and employees of PEFC Switzerland who process personal data within the scope of the performance of their functions and tasks.

It also applies to external persons and companies, provided that they undertake to comply with it by means of a corresponding written agreement.

5. Objective

The main objective of this concept is to ensure the protection of the privacy of natural persons against unlawful or disproportionate processing of personal data in accordance with section 1. As a binding guideline, this concept is intended to support all persons working at PEFC Switzerland in acting on their own responsibility in accordance with data protection law.

By implementing this objective, PEFC Switzerland also avoids material disadvantages and damage to its image that could arise due to acts contrary to data protection.

6. Principles of data protection

6.1. Legality

Data processing is lawful if it is justified by the consent of the data subject, a legal authorization or an overriding public or private interest.

6.2. Proportionality

The data collection must be necessary, and there should also be an overriding interest in the collection. Retaining data is illegal, data that is no longer needed must be destroyed.

6.3. Earmarking

The data may only be processed for the purpose stated when the data was collected. Your data may not be processed for any purpose that is not recognizable to the data subject.

6.4. Transparency

The collection and processing of data must be clearly recognizable. The necessary information should be obtained directly from the person concerned.

6.5. Quality

It must be ensured that the processed data is correct, complete and up-to-date. Incorrect and incomplete data must be corrected or destroyed.

6.6. Good faith

Contradictory and abusive behavior is not permitted.

7. Data Security: Measures

Organizational and technical measures are intended to ensure data protection and protect personal data, in particular from unauthorized access, misuse, destruction, loss, technical errors, forgery, theft, etc. be protected.

7.1. Organizational measures

Access to personal data at PEFC Switzerland is based on the principle of "as much as necessary, as little as possible".

The data protection officer, in cooperation with the relevant managers, therefore regulates for each data collection who has access to personal data under what conditions and how this is monitored. He/she keeps a register of processing activities in accordance with the legal requirements and keeps it up to date.

He/she also regulates who is granted access to archived data.

7.2. Technical measures

The protection of electronically processed data is ensured in particular by the use and regular comprehensive encryption, the use of firewalls, virus protection programs, etc. and the logging of accesses.

Access and personal data carrier controls prevent unauthorized persons from gaining access to databases or modifying, destroying, stealing, etc.

7.3. Archiving

Personal data that is no longer required for processing is processed in accordance with the guidelines of the data protection officer and archived for the defined duration.

7.4. Annihilation

Data of minor importance will be destroyed (physically destroyed or electronically irretrievably deleted) immediately after the purpose of processing has been achieved. The data protection officer determines the details.

8. Rights of data subjects

The following instructions serve the goal of handling situations that regularly occur in everyday life in a correct manner in terms of data protection law.

8.1. Enlightenment/Orientation

Clients and employees are informed about their data protection rights and obligations upon entry. The data protection officer will then inform you appropriately about the acquisition of personal data concerning you.

8.2. Right to information/inspection

The person affected by the processing of his or her data may request information about the collection, origin, content, purpose, category and legal basis and to inspect the data collection. It also has the right to disclose the parties involved in the collection and data recipients.

The person requesting information or inspection must identify himself/herself.

The information must be provided within 30 days in a generally understandable manner, in writing and free of charge.

The provision of information and the rights of inspection may exceptionally be restricted or denied if there are important and overriding public interests or particularly sensitive interests of third parties to the contrary.

If there is a risk that the person concerned (especially minors) could be exposed to too much burden with the provision of information or inspection, he or she may appoint another person to whom information or insight will be provided or granted access in his or her place.

8.3. Right to rectification

Unlawful or incorrectly processed as well as incorrect data must be corrected or destroyed.

8.4. Blocking/refusal to disclose data

Any data subject can have the disclosure of his or her data blocked if he or she can prove an interest worthy of protection. This does not apply if the disclosure of data constitutes a legal obligation, is necessary due to the overriding interests of third parties or is necessary for the clarification of alleged abusive acts of the data subject.

9. Instructions for action

The following instructions serve the goal of ensuring that situations that occur regularly in everyday life are handled correctly under data protection law:

9.1. How to behave in response to telephone and written enquiries

Personal data may not be passed on to outsiders without the express consent of the data subject or without the corresponding legal permission.

In the case of telephone enquiries, the clear identification of the inquiring person must be ensured. If telephone conversations are recorded, this must be pointed out and the consent of the interlocutor must be obtained.

9.2. Principles of e-mail use

E-mails can be read or changed by third parties. In principle, therefore, as little personal data as possible should be transmitted by e-mail and should not contain any sensitive information or information about passwords and other access data.

As a matter of principle, particularly sensitive data may only be transmitted by e-mail in encrypted form, unless the data subject has made a written declaration to the contrary.

Personal data processed for professional purposes may not be stored on private devices.

In addition, the regulations in the regulations of PEFC Switzerland on the use of computer science must also be observed.

9.3. Use of image/sound recordings

Recognizable on image, film and/or sound recordings, only persons who have given their consent may be detained.

The consent of the data subject must be voluntary, explicit and after prior information about the purpose and use of the recordings. Consent can be given in writing or – if several people are present – orally or non-verbally and must be documented.

10. Responsibilities

10.1. Board

Together with the managing director, the board is responsible for ensuring data protection at PEFC Switzerland at a strategic level.

It includes data protection as a relevant topic in its risk management system and assesses the corresponding risks in a strategically appropriate manner.

It issues this data protection concept and reviews it regularly.

10.2. Management

The management is responsible for the implementation of this concept and for compliance with the data protection requirements in the context of all data processing at the operational level.

It shall ensure in an appropriate manner that all employees are regularly sensitised to data protection issues and informed about the requirements of this concept and their application in their daily work.

10.3. Employees

All employees of PEFC Switzerland who process personal data shall take data protection into account on their own responsibility and shall act in particular in accordance with the present concept and the directives of Board or the Management.

If they have any questions, they shall contact the board or the management.

Appendix 1

<i>Personal</i>	Information about an identified or identifiable natural person.
<i>Particularly sensitive personal data</i>	<ul style="list-style-type: none"> a) data on religious, philosophical, political or trade union views or activities; b) data on health, privacy or membership of an ethnic group or origin; c) genetic data; d) biometric data that uniquely identifies a natural person; e) data relating to administrative and criminal prosecution or sanctions; f) Data on social assistance measures.
<i>Processing of personal data</i>	Any handling of personal data, regardless of the means and procedures used, such as procuring, storing, using, modifying, disclosing it, archiving, deleting or destroying data.
<i>Disclosure of personal data</i>	Any transmission or making available of personal data.
<i>Data collection</i>	Inventory of personal data that is structured in such a way that the data can be accessed according to specific persons.
<i>Data Protection Officer</i>	Person who monitors compliance with data protection regulations in-house and, among other things, keeps a register of data collections.
<i>Owner of the data collection</i>	Responsible for data processing. He/she decides alone or together with others on the purpose and means of processing.
<i>Personality profile</i>	Compilation of data that allows an assessment of essential aspects of the personality of a natural person.
<i>Profiling</i>	Evaluation of certain characteristics of a person on the basis of automatically processed personal data (e.g. to analyse or predict work performance, economic circumstances, health, behaviour, certain preferences, location or mobility).