Data protection policy for employees and officials of Swiss Hockey

Status:	Approved Secretary General 7.3.25
Valid from:	8. 3.25
Responsible:	Nick Zepf, Secretary General

1. Initial situation

Swiss Hockey is committed to ensuring the privacy and protection of its employees' personal data. This Privacy Policy explains how employees' personal data is collected, processed, and protected and ensures that processing is carried out in compliance with the Swiss Data Protection Act (DPA) and, where applicable, the EU General Data Protection Regulation (GDPR).

2. Scope

This privacy policy applies to all employees and officials of Swiss Hockey.

Directive No. 10 Data Protection applies in its current version.

This Privacy Policy specifies the relevant documents.

3. Data protection officer

The data protection officer is the Secretary General. His deputy is the Managing Director. Employees and officials can contact the above-mentioned persons at any time if they have any questions or concerns.

4. Principles

The following principles apply to daily work:

- Only data necessary for Swiss Hockey's work is collected.
- Data of all kinds (internal and external) may only be shared if necessary for daily work. Sharing in advance or nice to know is not permitted.
- Data must be regularly checked for accuracy. The person responsible for the specific data is always responsible for this.
- Data processing
    - The software used must always be kept up to date (always run updates)
    - Access authorization to systems and storage must be strictly managed and documented. Only those who need access should be granted access.

  - Access to systems must always be password-protected. Except for the public area of the homepage.
  - Data that requires particular protection must be encrypted during transmission.
  - Regular backups of all systems are required. They must be set up in such a way that they are not infected in the event of a ransomware attack.
  - If new software or a new IT system is used, the data protection officer must be informed in advance and his consent obtained.
- Deleting data
  - Data that we need for our daily work and data that we need by law may not be deleted.
  - Data that is no longer needed must be deleted. Before the data is deleted, the consent of the data protection officer or his or her representative must be obtained.
- Particularly sensitive data is primarily medical data. If such data is used, a processing directory must be created (who has access, on which system is it stored). If particularly sensitive data must be shared, the data protection officer or their representative must give prior approval. The data must be shared in encrypted form.

5. training

Each employee and official is familiarized with the data protection concept and the data protection policy when they are introduced to their new role (training).

6. Reporting obligation

If employees and officials discover a breach of data security or that there is a gap in data security, they are obliged to immediately inform the data protection officer or his deputy.