Datenschutzrichtlinie für Mitarbeitende und Funktionäre von Swiss Hockey

Status:	Genehmigt Generalsekretär 7.3.25
Gültig ab:	8.3.25
Verantwortlich:	Nick Zepf, Generalsekretär

1. Ausgangslage

Swiss Hockey verpflichtet sich, die Privatsphäre und den Schutz personenbezogener Daten seiner Mitarbeitenden zu gewährleisten. Diese Datenschutzrichtlinie erläutert, wie personenbezogene Daten von Mitarbeitenden erhoben, verarbeitet und geschützt werden, und stellt sicher, dass die Verarbeitung im Einklang mit dem Schweizer Datenschutzgesetz (DSG) und gegebenenfalls der EU-Datenschutz-Grundverordnung (DSGVO) erfolgt.

2. Geltungsbereich

Diese Datenschutzrichtlinie gilt für alle Mitarbeitenden und Funktionäre von Swiss Hockey.

Es gilt die Weisung Nr. 10 Datenschutz in der aktuellen Fassung.

Die vorliegende Datenschutzrichtlinie konkretisiert die relevanten Dokumente.

3. Verantwortlicher Datenschutz

Der Verantwortliche Datenschutz ist der Generalsekretär. Sein Stellvertreter ist der Geschäftsführer. Bei Fragen und Unklarheiten können sich die Mitarbeitenden und die Funktionäre jederzeit an die oben genannten Personen wenden.

4. Grundsätze

Für die tägliche Arbeit gelten die folgenden Grundsätze:

- Es werden nur jene Daten erhoben, die für die Arbeit von Swiss Hockey notwendig sind.
- Daten aller Art (intern und extern), dürfen nur weitergegeben werden, wenn dies für die tägliche Arbeit notwendig ist. Weitergabe auf Vorrat oder nice to know ist nicht gestattet.

- Daten sind regelmässig auf Korrektheit zu prüfen. Dafür verantwortlich ist immer jene Person, die für die spezifischen Daten verantwortlich ist.
- Datenverarbeitung
    - Die verwendete Software ist immer auf dem neusten Stand zu halten (Updates immer ausführen)
    - Die Zugriffsberechtigung auf Systeme und Ablagen ist restriktiv zu handhaben und zu dokumentieren. Nur wer Zugriff braucht, soll Zugriff bekommen.
    - Der Zugriff auf Systeme ist immer mit einem Passwort zu schützen. Ausnahme Homepage öffentlicher Bereich.
    - Besonders schützenswerte Daten sind bei der Übermittlung zu verschlüsseln.
    - Von allen Systemen ist regelmässig ein Backup notwendig. Sie müssen so aufgesetzt werden, dass sie bei einem Ransomware Angriff nicht infiziert werden.
    - Wenn eine neue Software oder ein neues IT-System eingesetzt wird, so ist vorgängig der Datenschutzbeauftragte zu informieren und seine Zustimmung einzuholen.
- Löschen von Daten
    - Daten, welche wir für unsere tägliche Arbeit brauchen sowie Daten, welche wir von Gesetzes wegen brauchen, dürfen nicht gelöscht werden.
    - Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Bevor die Daten gelöscht werden, muss vorgängig die Zustimmung des Datenschutzbeauftragten oder seines Stellvertreters eingeholt werden.
- Besonders schützenswerte Daten sind primär medizinische Daten. Wenn solche verwendet werden, dann muss dazu ein Bearbeitungsverzeichnis erstellt werden (Wer hat Zugriff, auf welchem System sind sie abgelegt). Wenn besonders schützenswerte Daten weitergegeben werden müssen, dann muss der Datenschutzbeauftragte oder sein Stellvertreter dem vorgängig zustimmen. Die Daten müssen verschlüsselt weitergegeben werden.

5. Schulung

Jeder Mitarbeitende und Funktionäre wird bei der Einführung in seine neue Aufgabe mit dem Datenschutzkonzept und der Datenschutzrichtlinie vertraut gemacht (Schulung).

6. Meldepflicht

Stellen Mitarbeitende und Funktionäre eine Verletzung der Datensicherheit fest oder dass eine Lücke in Bezug auf die Datensicherheit besteht, so ist er umgehend verpflichtet, den Datenschutzbeauftragten oder seinen Stellvertreter zu informieren.