Politique de protection des données pour les employés et les officiels de Swiss Hockey

Statut :	Approuvé par le Secrétaire général le 7.3.25
Valable à partir du :	8. 3.25
Responsable :	Nick Zepf, Secrétaire général

1. Situation initiale

Swiss Hockey s'engage à garantir la confidentialité et la protection des données personnelles de ses employés. Cette politique de confidentialité explique comment les données personnelles des employés sont collectées, traitées et protégées et garantit que le traitement est effectué conformément à la loi suisse sur la protection des données (DSG) et, le cas échéant, au règlement général sur la protection des données de l'UE (RGPD).

2. Portée

Cette politique de confidentialité s'applique à tous les employés et responsables de Swiss Hockey.

La Directive n° 10 sur la protection des données s'applique dans sa version actuelle.

Cette politique de confidentialité précise les documents pertinents.

3. Délégué à la protection des données

Le responsable de la protection des données est le Secrétaire général. Son adjoint est le directeur général. Si vous avez des questions ou des préoccupations, les employés et les fonctionnaires peuvent contacter les personnes mentionnées ci-dessus à tout moment.

4. Principes

Les principes suivants s'appliquent au travail quotidien :

- Seules les données nécessaires au travail de Swiss Hockey sont collectées.
- Les données de toutes sortes (internes et externes) ne peuvent être transmises que si cela est nécessaire au travail quotidien. Transmission de stock ou de bien à savoir n'est pas autorisé.
- L'exactitude des données doit être vérifiée régulièrement. La personne responsable des données spécifiques en est toujours responsable.

- Informatique
  - Le logiciel utilisé doit toujours être tenu à jour (toujours exécuter les mises à jour)
  - Les autorisations d'accès aux systèmes et aux fichiers doivent être traitées de manière restrictive et documentées. Seuls ceux qui ont besoin d'y accéder devraient y avoir accès.
  - L'accès aux systèmes doit toujours être protégé par un mot de passe. Exception : espace public de la page d'accueil.
  - Les données nécessitant une protection particulière doivent être cryptées lors de leur transmission.
  - Des sauvegardes régulières de tous les systèmes sont nécessaires. Ils doivent être configurés de manière à ne pas être infectés en cas d'attaque par ransomware.
  - Si un nouveau logiciel ou un nouveau système informatique est utilisé, le délégué à la protection des données doit en être informé au préalable et son consentement doit être obtenu.
- Suppression des données
  - Les données dont nous avons besoin pour notre travail quotidien et les données dont nous avons besoin en vertu de la loi ne peuvent pas être supprimées.
  - Les données qui ne sont plus nécessaires doivent être supprimées. Avant la suppression des données, le consentement du délégué à la protection des données ou de son suppléant doit être obtenu.
- Les données particulièrement dignes d'être protégées sont avant tout les données médicales. Si de tels fichiers sont utilisés, il faut alors créer un répertoire d'édition (qui y a accès, sur quel système ils sont stockés). Si des données particulièrement sensibles doivent être transmises, le délégué à la protection des données ou son suppléant doit donner son consentement préalable. Les données doivent être transmises sous forme cryptée.

5. Entraînement

Chaque employé et officiel est familiarisé avec le concept de protection des données et la politique de protection des données lors de son introduction à son nouveau rôle (formation).

6. Obligation de déclaration

Si les employés et les officiel découvrent une violation de la sécurité des données ou qu'il existe une lacune dans la sécurité des données, ils sont tenus d'en informer immédiatement le délégué à la protection des données ou son adjoint.