INFORMATIONS SUR LA NOUVELLE LOI SUR LA PROTECTION DES DONNÉES

DÈS LE 1ER SEPTEMBRE 2023

swiss aquatics

TABLE DES MATIÈRES

1. GÉNÉRALITÉS

La protection des données porte sur l'utilisation transparente et proportionnée des données personnelles et de leur traitement par les particuliers (personnes physiques et morales) et les autorités.

Par traitement, on entend toute manipulation d'informations, comme la collecte, la conservation, l'utilisation, l'exploitation, la communication ou la destruction. Même si des données personnelles reposent sur un support de stockage sans que vous les utilisiez de quelle sorte que ce soit, cela est considéré comme un traitement.

Les données personnelles sont des données telles que le nom, l'adresse, le numéro de téléphone, le numéro AVS, la date de naissance, etc. qui se rapportent à une personne physique spécifique ou identifiable.

Données personnelles particulièrement sensibles :

- origines raciales et ethniques
- opinions politiques, appartenance à un syndicat
- convictions religieuses ou idéologiques
- données génétiques
- données biométriques pour une identification sans équivoque
- Données de santé
- Données relatives à la vie sexuelle ou à l'orientation sexuelle
- En Suisse, en plus :
    - données relatives aux poursuites ou sanctions administratives et pénales,
    - données sur les mesures d'aide sociale

Pour les données personnelles particulièrement sensibles, il faut impérativement veiller à tenir un registre des traitements et à obtenir un consentement explicite - de préférence par écrit.

1.1. PRINCIPES DE TRAITEMENT

Les traitements de données sont toujours autorisés tant que les principes de traitement sont respectés :

1.1.1. LICÉITÉ ET BONNE FOI

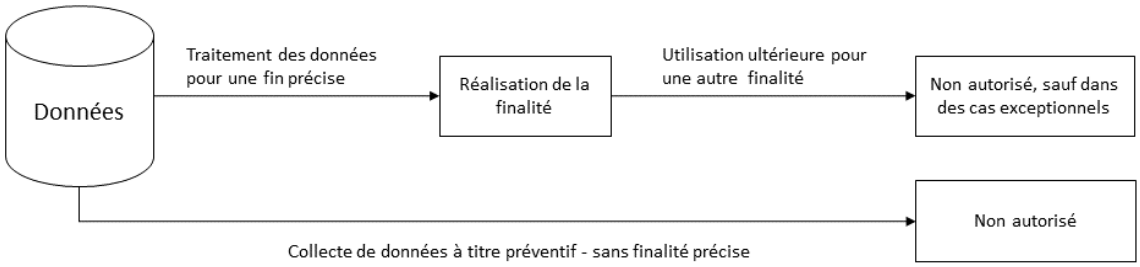
Les traitements de données ne peuvent être autorisés que s'ils sont licites et ne contreviennent pas au principe de la bonne foi.

Un traitement de données est licite lorsqu'il ne contrevient pas aux prescriptions légales. Notamment lorsque les principes de traitement expliqués ci-après sont respectés ou lorsqu'il existe un motif justificatif pour le traitement.

Le principe de la bonne foi est considéré comme respecté lorsque le comportement du responsable des relations juridiques est loyal. et digne de confiance. Il y a infraction en cas de comportement abusif de la part du responsable. Par exemple, lorsque le responsable induit une personne en erreur pour collecter ses données.

1.1.2. FINALITÉS

Les données personnelles ne peuvent être utilisées que dans le but pour lequel elles ont été collectées.



1.1.3. PROPORTIONNALITÉ (« MINIMISATION DES DONNÉES »)

Les données personnelles ne peuvent être traitées que si leur traitement est proportionné. Un traitement de données est proportionné lorsqu'il **est approprié**, **nécessaire** et **adéquat**.

- **Appropriation** - Le traitement est approprié pour atteindre l'objectif du traitement.
- **Nécessité** - Le but du traitement ne peut pas être atteint avec un traitement de données moins important. Les données des membres qui ont quitté la fédération doivent être supprimées dans la mesure où elles ne sont plus nécessaires.
- **Adéquation** - Le traitement est adéquat lorsqu'il existe un rapport raisonnable entre l'objectif du traitement et le traitement.

1.1.4. EXACTITUDE DES DONNÉES

Les données personnelles doivent être exactes et mises à jour. Elles doivent en outre être complètes.
Le responsable est tenu de vérifier régulièrement les données et, le cas échéant, de les effacer ou de les modifier.
corriger.

1.2. JUSTIFICATIONS

Si les principes de traitement ne sont pas respectés, le traitement des données est néanmoins autorisé si une justification peut être présentée :

Consentement de la personne concernée - Pour que le consentement soit valable, il faut que la personne concernée exprime sans ambiguïté son accord au traitement des données. Le consentement doit se référer à des objectifs précis
Pour les données personnelles particulièrement sensibles, le consentement doit être explicite.

> Exemple : un patient consent au traitement de ses données de santé à des fins de recherche en cochant activement la question correspondante sur le formulaire d'enregistrement à l'hôpital.

Exécution d'un contrat - Les traitements de données sont parfois nécessaires à l'exécution d'un contrat. Ils sont nécessaires si le contrat ne peut être exécuté sans le traitement des données.
Exemple : une personne commande un article de merchandising au club. Le club peut alors transmettre l'adresse de la personne à la Poste afin que celle-ci puisse lui envoyer l'article commandé par courrier.

Obligation légale - Les responsables ont des obligations légales de traitement des données personnelles. C'est notamment le cas des obligations de conservation ou de l'obligation de déclarer les données salariales aux assurances sociales.
Exemple : la fédération communique à son institution de prévoyance le salaire annuel d'un collaborateur.

Intérêts vitaux - Il s'agit d'un cas exceptionnel qui s'applique lorsqu'une personne dont la vie est menacée n'est pas en mesure de consentir à un traitement de données d'importance vitale.
Exemple : un athlète est victime d'un grave accident de sport et ne peut plus répondre. A l'hôpital, ses données personnelles sont néanmoins traitées afin qu'il puisse être soigné.

Intérêts prépondérants - Si les intérêts du privé dans un traitement de données l'emportent sur les intérêts de la personne concernée, une justification est donnée. Cette justification ne peut être invoquée que dans un cadre limité et exige toujours une pesée des intérêts.
Exemples :

- Un club procède à une vérification de la solvabilité d'un membre potentiel
- Un club fait du marketing direct auprès de ses membres

2. RESPONSABILITÉS

2.1. RÔLES

2.1.1. RESPONSABLE (APPELÉ CONTROLLER)

- « Décide », conjointement avec d'autres ou seul, « des finalités et des moyens » (traitement matériel ou automatisé, logiciel utilisé) du traitement des données personnelles.
- Doit veiller à ce qu'un traitement de données réponde aux exigences légales et assume la responsabilité si tel n'est pas le cas.

Le Controller est responsable :

- De la licéité du traitement

- Des finalités
- Du devoir d'information lors de la collecte de données personnelles
- De la minimisation des données
- Du respect des droits des personnes concernées
- De la sélection de processeurs appropriés
- Du respect des directives en cas d'une communication transfrontière
- De la sécurité de l'information
- De l'annonce de toute violation de la protection des données
- De la coopération avec l'autorité de surveillance (PFPDT)
- Du rendement de compte et du respect des règles de conservation
- Le cas échéant, de l'évaluation de l'impact sur la protection des données,
- Le cas échéant, de la tenue du registre des traitements
- Le cas échéant, de la nomination d'un conseiller en matière de protection des données,

2.1.2. PERSONNE EN CHARGE DU TRAITEMENT DES DONNÉES (APPELÉ PROCESSOR)

- Exécute le traitement pour le compte du responsable.
- Doit traiter les données selon les instructions de son client.
- Accord sur les traitements des données (ATD)
    - Objet et étendue du traitement des données
    - Responsabilités
    - Finalités des données

2.2. OBLIGATION D'INFORMATION

Le responsable informe de manière appropriée la personne concernée de la collecte de données personnelles ; ce devoir d'information s'applique également lorsque les données sont collectées auprès d'un tiers (cf. art. 19 nLPD).

Sous quelle forme et dans quel délai l'information est-elle donnée ? en général dans une déclaration de protection des données, au plus tard un mois après avoir reçu les données d'un tiers (plus tôt si elles sont communiquées)

Par exemple, en cas d'achat d'adresses ou de reprise de données d'adresses d'un club qui se dissout.

3. SÉCURITÉ DES DONNÉES

La sécurité des données est le fondement d'une protection efficace des données. Elle protège les données contre toute forme de perte, de vol ou de manipulation. C'est pourquoi la loi sur la protection des données

impose des exigences élevées en matière de sécurité des données. Les objectifs de protection légaux suivants doivent être atteints :

- Confidentialité
- Disponibilité
- Intégrité
- Traçabilité

3.1. MESURES TECHNIQUES ET ORGANISATIONNELLES

Approche basée sur les risques
Pour atteindre les objectifs de protection, des mesures techniques et organisationnelles (appelées « TOM ») doivent être prises. Les exigences posées aux TOM sont déterminées en fonction du risque lié à chaque traitement de données et du besoin de protection des données traitées.

- **Plus le risque et le besoin de protection sont élevés, plus les exigences en matière de TOM sont importantes.**

L'état actuel de la technique et les coûts de mise en œuvre peuvent être pris en compte lors de la définition des TOM nécessaires.

3.2. SÉCURITÉ DES DONNÉES

- **Confidentialité**

Les données personnelles ne doivent être **accessibles** qu'**aux personnes autorisées**. Le cercle des personnes autorisées est déterminé par le **contexte du domaine d'activité** ainsi que par le contenu et l'importance des données. Il peut être très large ou extrêmement restreint.

Par confidentialité, on entend également l'**authentification**, les méthodes qui y sont liées ainsi que les systèmes de **gestion et de restriction d'accès** pour garantir la sécurité des données.

- **Disponibilité**

Le responsable veille à ce que les données puissent **être consultées à tout moment**. Cette exigence est d'autant plus élevée lorsque les informations doivent être disponibles en permanence pour l'exécution de tâches essentielles, voire légales.

- Intégrité

L'exactitude des données doit être garantie. Elle est particulièrement importante lorsque les données sont destinées au public ou doivent être réutilisées. Par intégrité, on entend l'authenticité, l'imputabilité et la non-répudiation des données.

- Sécurité du système

Il n'est pas exigé que chaque mise à jour du système et des applications soit installée immédiatement, mais qu'un processus de mise à jour soit en place (appelé Vulnerability- and Patchmanagement).

La mise à jour de sécurité correspondante peut être mise en œuvre de manière échelonnée dans le temps, en tenant compte des niveaux de criticité (élevé, moyen, faible).

Mais jusqu'à ce que les points faibles soient corrigés, des mesures doivent être prises pour que la sécurité des données reste tout de même garantie.

Il ne s'agit pas de mesures réactives, mais de l'élimination proactive des points faibles pour lesquels aucune violation de la sécurité des données n'a été constatée jusqu'à présent dans le système.

- Traçabilité

Les accès non autorisés, voire les abus, doivent pouvoir être identifiés. En outre, la cause d'un incident peut être déterminée. Le responsable veille à l'enregistrement des événements et des traces de données et s'assure que celles-ci ne peuvent pas être modifiées. La traçabilité du traitement peut être importante pour la procédure (preuves) et facilite les contrôles et la surveillance.

Contrôle de la saisie - Quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé des données, à quel moment et par quelle personne ?

Contrôle de la communication - à qui les données personnelles sont communiquées à l'aide de dispositifs de transmission de données

Détection - les violations de la sécurité des données doivent être rapidement détectées

Élimination - Des mesures doivent pouvoir être prises pour réduire ou éliminer les conséquences.

Mise en œuvre de deux mesures supplémentaires lorsque des données personnelles particulièrement sensibles (par ex. des données relatives à la santé) sont traitées à grande échelle ou lorsqu'un Profiling à haut risque est effectué :

- Enregistrement dans le système (saisie et conservation des logs)
- Tenue d'un règlement de traitement

3.3. MESURES GÉNÉRALES

En outre, il existe encore quelques mesures qui sont toujours utiles, indépendamment du traitement concret des données :

- Procéder à des mises à jour régulières des logiciels et des systèmes
- Sensibilisation et formation des collaborateurs, des organes et des auxiliaires
- Gestion des autorisations
- Gestionnaire de mots de passe et authentification à deux facteurs
- Bien organiser les sauvegardes pour qu'elles ne soient pas infectées par un ransomware en cas de cyberattaque
- Cryptage des données sensibles lors de leur transmission
- N'autoriser le BYOD (Bring Your Own Device) que de manière restrictive

4. DÉCLARATION OBLIGATOIRE

En cas de violation de la sécurité des données, une notification au PFPDT doit être effectuée s'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'information est également transmise à la personne concernée si cela est nécessaire à sa protection ou si le PFPDT l'exige (cf. art. 24 nLPD).

La notification doit être effectuée le plus rapidement possible.

Contenu de la notification : le type de violation de la sécurité des données, ses conséquences et les mesures prises ou prévues

5. DROITS DES PERSONNES CONCERNÉES

5.1. DROIT D'ACCÈS

Toute personne peut demander au responsable les informations suivantes :

- Savoir si des données personnelles les concernant sont traitées
- Et si oui, lesquelles.

La loi précise le contenu minimal de l'information :

- Informations sur l'identité et les coordonnées du responsable
- Finalités du traitement
- Durée de conservation (ou ses critères)
- Source des données (si disponible)
- Décisions individuelles automatisées (et logique)
- Catégories de destinataires (par ex. autorités)
- Informations sur l'exportation des données
- Clause générale

5.1.1. DÉROULEMENT

- La personne doit faire une demande écrite accompagnée d'une copie valable de sa pièce d'identité (CI / passeport).
- Consultation interne avec le responsable
- En règle générale, les renseignements doivent être fournis dans les 30 jours.
- En cas de charge de travail disproportionnée, un montant de 300 CHF sera facturé au demandeur.

Refus, restriction, report de l'information

Secret professionnel, intérêts prépondérants de tiers, la demande est manifestement quérulente, la demande poursuit un but contraire à la protection des données (préparation de procès). Le motif doit être indiqué.

5.2. SUPPRESSION ET RECTIFICATION

Les données personnelles doivent être détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires au but du traitement (al. 4).

Quiconque traite des données personnelles doit s'assurer de leur exactitude. Il doit prendre toutes les mesures raisonnables pour que soient rectifiées, effacées ou détruites les données qui sont inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ou traitées (al. 5).

5.3. DROIT À LA RESTITUTION DES DONNÉES

La personne concernée peut demander au responsable de lui restituer ses données personnelles ou de les faire transférer à un tiers.

- L'objectif de la restitution des données est de permettre à la personne concernée de faire transférer directement ses données à une nouvelle personne responsable.
- Ainsi, la personne a plus de contrôle sur ses données (par exemple en cas de changement de club).

6.TRANSFERT DE DONNÉES À L'ÉTRANGER

Exportations de données
Dès que des données personnelles sont traitées en rapport avec l'étranger, il y a exportation de données.

Les exportations de données sont soumises à des règles particulières (selon le pays destinataire) auxquelles les exportateurs doivent se conformer.

Exemple 1 :
Un club sportif envoie un e-mail contenant des données personnelles à l'organisateur d'une compétition à l'étranger.

- Il y a exportation de données, car les données personnelles sont transmises à l'étranger.

Exemple 2 :
Un club sportif stocke les données de ses membres sur un cloud dont les serveurs sont situés à l'étranger.

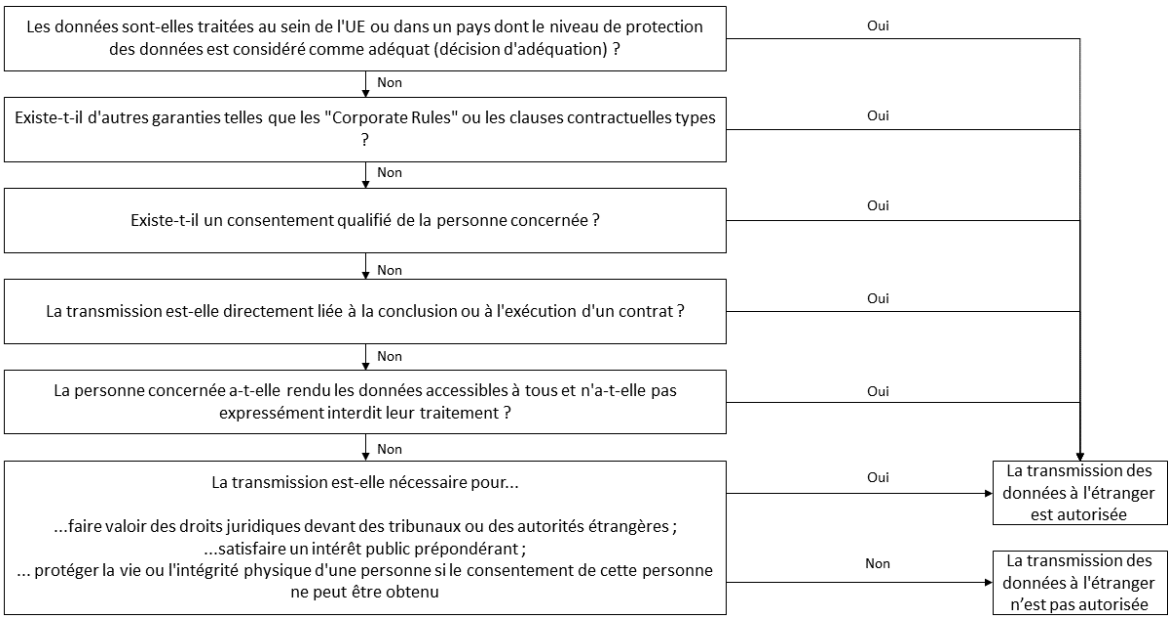
- Si des données personnelles sont stockées à l'étranger, cela est également considéré comme une exportation de données.

- Il y a également exportation lorsqu'il est possible d'accéder aux données depuis l'étranger (par exemple en cas de support).

Les données peuvent être exportées sans problème dans les pays qui présentent un niveau de protection des données adéquat.

La liste des Etats disposant d'un niveau de protection des données adéquat est décidée par le Conseil fédéral et peut être consultée sous https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html#-2053327153.

Si un pays vers lequel des données doivent être exportées ne présente pas un niveau de protection des données adéquat, les données ne peuvent être exportées que sous certaines conditions (voir graphique).



Lorsque des pays, comme les **États-Unis**, ne présentent pas un niveau de protection des données adéquat, la solution la plus simple consiste à conclure des clauses contractuelles types avec l'importateur de données. Les clauses contractuelles types sont contraignantes tant pour l'exportateur de données que pour l'importateur de données. Elles garantissent que les données sont traitées conformément à la loi.

Les clauses contractuelles types obligent l'exportateur de données à établir un « Transfer Impact Assessment » (TIA). Le TIA doit déterminer si les données personnelles sont exposées dans le pays destinataire à d'éventuels risques liés aux autorités locales. Si un risque élevé est constaté, celui-ci doit être neutralisé par des mesures techniques et organisationnelles.

Modèle de TIA : https://iapp.org/resources/article/transfer-impact-assessment-templates/