FÉDÉRATION QUÉBÉCOISE POUR LE SAUMON ATLANTIQUE

Politique relative à la gouvernance des renseignements personnels

Adoptée par le conseil d'administration
8 décembre 2023

TABLE DES MATIÈRES

1. OBJECTIFS DE LA PRÉSENTE POLITIQUE

Le conseil d'administration de la Fédération québécoise pour le saumon Atlantique (FQSA) a la volonté et l'obligation légale de se doter de pratiques sécuritaires afin d'assurer la confidentialité des informations personnelles que l'association obtient, détient et utilise dans le cadre de ses opérations. Ces pratiques incluent aussi la destruction des informations personnelles.

La présente politique de gouvernance des données définit les principes et les pratiques qui guident la collecte, l'utilisation et la gestion des données par la FQSA. Elle mentionne les rôles et responsabilités, des directives techniques et comportementales pour la qualité, l'intégrité, la sécurité, la confidentialité, la conformité, la conservation et l'archivage des données.

2. DÉFINITIONS

- Données : Toute information stockée, collectée, traitée ou utilisée, quel que soit le format ou le support utilisé.
- Gouvernance des données : Ensemble des politiques, des normes, des procédures et des rôles pour gérer les données de manière responsable et éthique.
- Renseignement personnel : Tout renseignement qui concerne une personne physique et permet de l'identifier.
- Renseignement personnel sensible : Selon la commission d'accès à l'information du Québec, un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attente raisonnable en matière de vie privée, en raison de sa nature ou du contexte de son utilisation.
- Incident de confidentialité : Selon la commission d'accès à l'information du Québec, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

3. RÔLES ET RESPONSABILITÉS

3.1. LE CONSEIL D'ADMINISTRATION

Le conseil d'administration a la responsabilité de superviser la gouvernance des données et de s'assurer que l'organisation utilise les données de manière responsable, éthique et sécurisée. La personne responsable du conseil d'administration doit compléter l'Annexe 1 – Formulaire de désignation – Personne responsable des renseignements personnels.

Responsabilités :

3.1.1 Le conseil d'administration doit s'assurer que des politiques encadrant la gestion des données sont mises en place au sein de l'organisme et doit s'assurer que les ressources nécessaires sont allouées à leur mise en œuvre.

3.1.2 Évaluer les risques liés aux données : Le conseil d'administration doit comprendre les risques liés à la collecte, au stockage et à l'utilisation des données de l'organisation et s'assurer que des mesures adéquates sont mises en place pour les

atténuer.

3.1.3 Surveiller la conformité réglementaire : Le conseil d'administration doit s'assurer que l'organisation est en conformité avec les lois et les règlements en matière de protection des données. Il doit également surveiller les développements réglementaires et s'assurer que l'organisation s'adapte en conséquence.

3.1.4 Assurer la transparence et la responsabilité : Le conseil d'administration doit s'assurer que les politiques de gouvernance des données de l'organisation sont clairement communiquées à tous les employés, parties prenantes et autres personnes concernées. Il doit également s'assurer que l'organisation est responsable de la gestion de ses données et est transparente dans ses activités liées aux données.

3.2. LE DIRECTEUR GÉNÉRAL/LA DIRECTRICE GÉNÉRALE (OU LA PERSONNE DESIGNÉE PAR LE CONSEIL D'ADMINISTRATION)

La directrice générale est désignée expressément par le conseil d'administration comme la personne responsable de l'accès aux informations personnelles et à la protection des renseignements personnels.

Les coordonnées de la directrice générale sont les suivantes :

DIRECTRICE GÉNÉRALE: Myriam Bergeron
COURRIEL : mbergeron@fqsa.ca
TÉLÉPHONE : 418 847 91 91

Si la directrice générale n'est pas disponible pour une période prolongée de plus de 30 jours et ne peut répondre à une demande d'accès à l'information, le président du conseil d'administration est désigné pour répondre et traiter la demande en son absence.

Responsabilités :

3.2.1 Surveiller la conformité réglementaire de l'OBNL aux lois et réglementations applicables en matière de protection des données, notamment la Loi 25 du Québec qui vise la protection des renseignements personnels.

3.2.2 Élaborer des politiques et des procédures pour assurer la protection des données personnelles de l'organisation. Ces politiques et procédures peuvent inclure des politiques de confidentialité, des procédures de contrôle d'accès et des protocoles de gestion des incidents.

3.2.3 Évaluer les risques liés à la collecte, au stockage et à l'utilisation des données de l'organisation et mettre en place des mesures pour les atténuer.

3.2.4 S'assurer que les mesures de sécurité appropriées sont en place pour protéger les données contre les accès non autorisés, les pertes ou les altérations.

3.2.5 Sensibiliser le personnel de l'organisation à l'importance de la protection des données personnelles et leur fournir des formations régulières pour s'assurer que les employés comprennent leur rôle dans la protection de la vie privée des personnes concernées.

3.2.6 Gérer les demandes d'exercice de droits des personnes concernées, telles que le

droit d'accès, de rectification ou de suppression de leurs données personnelles.

3.2.7 Répondre aux demandes d'accès à l'information et de traiter ces demandes en conformité avec la Loi et la présente politique.

3.2.8 Protéger les données contre l'accès non autorisé, la divulgation ou la perte en utilisant des mesures de sécurité appropriées.

3.2.9 Signaler tout problème lié aux données, y compris les violations de données ou les préoccupations de sécurité, au responsable de la gouvernance des données de l'organisme.

3.3. LES EMPLOYÉS ADMINISTRATIFS

Les employés administratifs sont responsables de la collecte de données en utilisant le logiciel Userboat de Spektrum. Ils doivent s'assurer que les données collectées sont pertinentes pour les objectifs de l'organisation. Ils doivent utiliser les données de manière responsable et appropriée, conformément aux lois et règlements applicables et aux politiques de l'OBNL en matière de données. Ils doivent également respecter les droits de confidentialité des personnes dont les données sont collectées.

Responsabilités :

3.3.1 Respecter les normes de confidentialité en matière de données et garantir que les données sont stockées et gérées de manière sécurisée.

3.3.2 Documenter les données de manière complète et précise.

3.3.3 Respecter les politiques de l'OBNL en matière de données, en veillant à ce que les données soient utilisées de manière responsable et appropriée et en garantissant que les données sont partagées de manière responsable et conforme aux lois et règlements applicables.

4. Directive

4.1. CONSENTEMENT

La FQSA s'engage à recueillir un consentement avant de recueillir les renseignements personnels d'un individu. Le consentement peut être explicite ou implicite et peut être fourni directement par la personne ou par son représentant autorisé.

L'obtention d'un consentement explicite, que ce soit verbalement, par voie électronique ou par écrit, est privilégié. Toutefois, le consentement implicite peut être raisonnablement déduit de l'action ou de l'inaction d'une personne. Par exemple, le fait de fournir un nom et une adresse pour recevoir une publication ou un nom et un numéro de téléphone pour obtenir une réponse à une question est considéré comme un consentement implicite à la collecte d'information contenant des renseignements personnels. Pour déterminer le type de consentement approprié, nous tenons compte de la sensibilité des renseignements personnels en cause, des fins auxquelles ils sont recueillis et des attentes raisonnables d'une personne placée en situation similaire. En cas de recueil d'informations personnels dites sensibles, nous nous engageons à faire remplir l'Annexe 4 – Formulaire de

consentement.

Si nous voulons utiliser les renseignements personnels à une nouvelle fin, nous décrirons l'utilisation prévue et demanderons à nouveau le consentement.

Il n'est pas toujours possible, notamment dans le cadre d'une demande de l'État, d'obtenir le consentement de la personne pour recueillir, utiliser ou communiquer ses renseignements personnels. Nous nous engageons à ne jamais communiquer ce type de renseignement, autrement qu'en conformité avec la présente Politique, sauf si la loi nous y oblige ou le permet.

4.2. RÉPERTOIRE DES RENSEIGNEMENTS PERSONNELS ET DÉLAIS DE CONSERVATION

À titre de prestataire de services, la FQSA doit recueillir plusieurs renseignements personnels. Ces renseignements personnels sont consignés par écrit sur des formulaires ou des ententes, et ce, par le biais de divers moyens technologiques.

D'une manière non limitative, voici la liste des renseignements personnels que FQSA doit recueillir, les fins de la collecte, les moyens utilisés ainsi que le délai de conservation de ceux-ci.

Relation	Type de renseignement personnel	Fin de la collecte	Moyens utilisés	Délais de conservation
Participants à	Les renseignements		• Sharepoint	• 5 ans

Relation	Type de renseignement personnel	Fin de la collecte	Moyens utilisés	Délais de conservation
des activités et événements, infolettre grand public	demandés ne comportent pas nécessairement la liste exhaustive, mais sont demandés en fonction des besoins de l'événement ou du moyen de communication : • Nom et prénom ; • Adresse postale (pays, province, ville, code postal, adresse) ; • Numéros de téléphone (domicile et cellulaire lorsqu'applicable) ; • Courriel ; • Renseignements bancaires ;	• Établir et gérer les relations avec la clientèle (et obtenir un moyen de communication). • Assurer le paiement des coûts liés aux services.	• Par téléphone • Par courriel • Lors de l'abonnement à l'infolettre (Mailchimp) • Formulaire papier	Réf. : BANQ Les renseignements bancaires lors de transactions électroniques ne sont pas conservés.
Membres ou administrateur de la FQSA.	• Nom et prénom ; • Adresse postale (pays, province, ville, code postal, adresse) ; • Numéros de téléphone (domicile et cellulaire lorsqu'applicable) ; • Date de naissance (facultatif) ; • Courriel ;	• L'inscription comme membre. • Les communications futures. • Établir et gérer les relations avec la clientèle (et obtenir un moyen de communication). • Assurer le paiement des coûts liés aux services.	• Spektrum Logiciel Userboat. • Par téléphone. • Par courriel. • Formulaire papier.	• 5 ans Réf. : BANQ Les renseignements bancaires lors de transactions avec le système d'adhésion des membres ne sont pas conservés.

Relation	Type de renseignement personnel	Fin de la collecte	Moyens utilisés	Délais de conservation
Employés	• Nom et prénom ; • Adresse postale (pays, province, ville, code postal, adresse) ; • Numéros de téléphone (domicile et cellulaire lorsqu'applicable) ; • Date de naissance ; • Courriel ; • Renseignements bancaires ; • Numéro d'assurance sociale ; • Dossier d'employé (bulletin de paie, évaluation, contrat de travail, etc.) ;	• La gestion des communications avec le candidat ou l'employé. • Assurer le fonctionnement du système de paie.	• Par courriel. • Par téléphone.	• 6 ans Réf. Loi sur l'équité salariale
Fournisseurs de services	• Nom et prénom ; • Numéro de téléphone ; • Courriel ; • Renseignements bancaires ;	• La gestion des mandats. • Le paiement des factures.	• Par courriel • Par téléphone • Par la poste	• 5 ans Réf. : BANQ

4.3. SAUVEGARDE ET RESTAURATION

La FQSA prend des mesures de sécurité propres à assurer la sécurité des renseignements compte tenu, notamment, de la sensibilité des renseignements, de leur finalité, de leur quantité et du support utilisé.

La directrice générale est responsable de la mise en place des mots de passe, de l'octroi des accès, et des diverses mesures informatiques, dont le système de sauvegarde « back-up » sécurisé.

La FQSA a recours aux services de fournisseurs de services tiers, notamment pour des services de marketing ainsi que l'hébergement et le stockage des informations recueillies. Notre site Web est hébergé au Québec, Canada et certaines données sont stockés par Mailchimp aux États-Unis. Afin de connaître les pratiques de Mailchimp relatives au traitement et au stockage des renseignements personnels, veuillez consulter les politiques du fournisseur au https://mailchimp.com/fr/legal/terms/. Le traitement des renseignements

personnels transférés à l'extérieur du Canada sera assujetti aux lois du pays où ces renseignements sont détenus.

4.4. CLASSIFICATION

La classification des données s'applique à toutes les données de l'organisation, quel que soit leur format (papier, électronique, etc.) ou leur emplacement (serveurs internes, services, infonuagiques, etc.). La classification des données se trouve dans le dictionnaire de données de l'organisme.

La FQSA adopte les niveaux de classification de données suivants :

1. Données confidentielles : Toute donnée qui, si elle était divulguée, pourrait causer un préjudice à l'organisme, à ses membres ou à ses parties prenantes. Les données confidentielles doivent être stockées dans des systèmes sécurisés et ne doivent être accessibles qu'aux personnes autorisées.
2. Données internes : Informations accessibles aux employés et aux non-employés autorisés (bénévoles, consultants et sous-traitants) qui ont besoin de les connaître à des fins professionnelles.
3. Données publiques : Toute donnée qui peut être librement partagée avec le public sans risque de préjudice pour l'organisation, ses membres ou ses parties prenantes. Les données publiques peuvent être diffusées librement.

4.5. ACCÈS AUX DONNÉES

La FQSA s'engage à limiter l'accès et l'utilisation des renseignements personnels aux personnes détenant les fonctions appropriées au sein de l'entreprise, et ce, seulement lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

La FQSA protège ses actifs de données grâce à des mesures de sécurité qui assurent un accès approprié aux données lorsqu'elles sont consultées. Chaque élément de données est classifié et approuvé par le responsable de la gouvernance des données pour avoir un niveau d'accès approprié. L'accès aux données sera effectué conformément aux politiques de sécurité.

4.6. UTILISATION DES DONNÉES

Les employés, les contractuels et les bénévoles doivent accéder aux données et les utiliser uniquement dans la mesure requise pour l'exécution de leurs fonctions, et non à des fins personnelles ou à d'autres fins inappropriées ; ils doivent également accéder aux données et les utiliser selon les niveaux de sécurité attribués aux données. Également, notre organisme ne détient aucun renseignement personnel concernant un mineur de moins de 14 ans, à moins de consentement du titulaire de l'autorité parentale ou du tuteur, sauf lorsque cette collecte sera manifestement au bénéfice de ce mineur.

L'utilisation des données est classée dans les catégories suivantes : mise à jour, lecture seule et diffusion externe.

1. Mise à jour : l'autorisation de mettre à jour les données doit être accordée par le responsable de la gouvernance des données de l'organisme (ou une personne responsable désignée) aux personnes dont les tâches spécifient et exigent la responsabilité de la mise à jour des données.
2. Lecture seule : l'accès en lecture seule doit être autorisé par le responsable de la gouvernance des données de l'organisme (ou une personne responsable désignée) aux personnes dont les tâches nécessitent l'accès aux données.
3. Diffusion externe : Toute divulgation des données doit être approuvée par le responsable de la gouvernance des données de l'organisme (ou une personne responsable désignée) et doit être guidée par la nécessité de respecter la vie privée individuelle et de protéger l'intégrité des données.

4.7. INCIDENT DE CONFIDENTIALITÉ

En cas d'accès, d'utilisation ou de communication non autorisée par la Loi ou par la personne concernée à un renseignement personnel ou la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement que la FQSA sur une ou des personne(s), la directrice générale doit :

- Aviser la Commission d'accès à l'information (CAI) si nous sommes en présence d'un risque de préjudice sérieux ;
- Aviser la personne visée par écrit. Pour ce faire, vous pouvez utiliser l'Annexe 3 – Modèle d'avis en cas d'incident de confidentialité.
- Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent ;
- Aviser toute personne ou tout organisme susceptible de diminuer ce risque (obligation de conserver une preuve)
- Tenir un registre des incidents de confidentialité. Un modèle est disponible en Annexe 2 – Registre des incidents de confidentialité.
- L'entreprise Spektrum, fournisseur de service, est responsable de la gestion des données. Spektrum s'est également dotée d'une politique de gouvernance des renseignements personnels. Les détails de cette politique sont disponibles auprès de l'entreprise.

5. APPLICATION

Cette politique doit être respectée par tous les employés, contractuels et bénévoles de la FQSA. La vérification de la conformité à cette politique est la responsabilité du responsable de la gouvernance des données de l'organisme. Les conséquences de la violation de cette politique dépendront des faits du cas, y compris la nature de la violation, l'existence de violations antérieures de cette politique ou d'autres politiques de l'organisme, la gravité de la violation et les lois applicables.

D'ailleurs, une communication a été acheminée aux membres de la FQSA (Annexe 5 – Lettre

d'informations aux membres), pour les informer de la conformité de l'organisation aux nouvelles normes de la loi 25.

6. POLITIQUE DE TRAITEMENT DES PLAINTES

Toute personne qui souhaite formuler une plainte relative à l'application de la présente politique ou, plus généralement, à la protection de ses renseignements personnels doit le faire par écrit en s'adressant au responsable de la protection des renseignements personnels, à l'adresse courriel : Info@fqsa.ca.

L'individu devra indiquer son nom, ses coordonnées pour le joindre, incluant un numéro de téléphone, ainsi que l'objet et les motifs de sa plainte, en donnant suffisamment de détails pour que celle-ci puisse être évaluée par la Fédération. Si la plainte formulée n'est pas suffisamment précise, le responsable de la protection des renseignements personnels peut requérir toute information additionnelle qu'il juge nécessaire pour pouvoir évaluer la plainte.

Toute plainte reçue sera traitée de façon confidentielle dans les 30 jours suivant la réception de celle-ci.

Dans le cas où la plainte ne peut être traitée dans ce délai, le plaignant doit être informé des motifs justifiant l'extension de délai, de l'état d'avancement du traitement de sa plainte et du délai raisonnable nécessaire pour pouvoir lui fournir une réponse définitive.

Il est également possible de déposer une plainte auprès de la Commission d'accès à l'information du Québec ou à tout autre organisme de surveillance en matière de protection des renseignements personnels responsable de l'application de la loi concernée par l'objet de la plainte. Toutefois, La Fédération invite toute personne intéressée à s'adresser d'abord à son responsable de la protection des renseignements personnels et à attendre la fin du processus de traitement à l'interne d'abord.

7. RÉFÉRENCES ET DOCUMENTS EXTERNES

- Aide-Mémoire : Résumé des nouvelles dispositions de la Loi 25 visant à protéger la vie privée des Québécois
- Le site internet de la commission d'accès à l'information
- La Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE)
- https://maloi25.ca