POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

SOCIÉTÉ D'HISTOIRE LES RIVIÈRES

SEPTEMBRE 2023

Politique interne de gouvernance des données (SHLR)

1 Introduction

La Loi 25 adoptée par l'Assemblée nationale en septembre 2021 (*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels)* reconnaît formellement qu'une entreprise ou un organisme est responsable de la protection des renseignements personnels qu'elle détient et ce, que leur conservation soit assurée par l'organisme ou par un tiers.

Cette politique de la Société d'histoire Les Rivières **(SHLR)** s'applique aux documents de tous formats (papier, numérique ou audiovisuel), qu'ils soient des fichiers enregistrés, des documents de travail, des documents électroniques, des courriels, des transactions en ligne, des données conservées dans des bases de données ou sur bande ou sur disque, des cartes, des plans, des photographies, des enregistrements sonores et vidéos.

2 Références et documents externes

- Aide-Mémoire : Résumé des nouvelles dispositions de la Loi 25 visant à protéger la vie privée des Québécois
- La Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE)
- Ministères et Organismes | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Modernisation de la protection des renseignements personnels | Gouvernement du Québec (quebec.ca)
- https://www.cai.gouv.qc.ca/documents/CAI_Guide_obligations_entreprises_vf.pdf
- P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé (gouv.qc.ca)

3 Définitions

- Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- Exemples de données personnelles : nom et prénom, adresse postale, adresse courriel, numéro de téléphone ou de cellulaire, âge ou date de naissance, genre, nationalité, etc.
- 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.

- Communication : Période où le renseignement personnel est communiqué à un tiers, par exemple dans un système de prestation électronique de services, par courriel ou par le biais de sites Web.
- Conservation : Période durant laquelle un organisme garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.
- Incident de confidentialité : accès non autorisé à un renseignement personnel, une utilisation ou communication non autorisé de celui-ci ou une perte pouvant causer un préjudice grave pour la personne concernée.

4 Rôles et responsabilités à la SHLR pour la gouvernance des données

4.1 Conseil d'administration de la SHLR

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.

Responsabilités:

4.1.1 S'assurer que des politiques encadrant la gestion des données sont mises en place au sein de l'organisme et soit s'assurer que les ressources nécessaires sont allouées à leur mise en œuvre.

4.1.2 Évaluer les risques liés aux données : 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.

4.1.3 Assurer la transparence des opérations : les politiques de gouvernance des données de l'organisation sont clairement communiquées à toutes les 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.

4.1.4 Déclarer tout incident sur la confidentialité : Les incidents de confidentialité ou toute atteinte aux renseignements personnels qui sont en la possession d'une organisation (accès non autorisé, utilisation ou communication non autorisée, ou perte pouvant causer un préjudice grave) doivent obligatoirement être déclarés à la Commission d'accès à l'information (CAI) et aux personnes touchées.

4.2 Responsable de la gouvernance des données

Le secrétaire de la SHLR est le responsable de la gouvernance des données pour l'organisme. Celui-ci est chargé de superviser et de garantir que l'organisme se conforme aux lois et réglementations applicables en matière de protection des données personnelles.

Responsabilités :

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

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

4.3 Créateurs de données

Les créateurs de données (ex. administrateurs) sont responsables de la collecte de données en utilisant des méthodes valides et fiables. Ils doivent s'assurer que les données collectées sont pertinentes pour les objectifs de la SHLR.

Responsabilités :

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

4.3.2 Documenter les données de manière complète et précise.

4.3.3 Respecter les politiques de la SHLR en matière de données, en veillant à ce que ces données soient utilisées de manière responsable et appropriée.

4.4 Utilisateur de données

Les utilisateurs de données (ex. membres) doivent utiliser les données de manière responsable et appropriée, conformément aux lois et règlements applicables et aux politiques de la SHLR en matière de données. Ils doivent également respecter les droits de confidentialité des personnes dont les données sont collectées.

Responsabilités :

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

4.4.2 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.

4.4.3 Respecter les politiques de la SHLR en matière de données, en veillant à ce que les données soient utilisées de manière responsable et appropriée.

5 Directives pour la gouvernance des données de la SHLR

5.1 Sécurité

L'utilisation personnelle des données de la SHLR, y compris les données dérivées, dans n'importe quel format et à n'importe quel endroit, est interdite.

Les dossiers stockés dans un format électronique doivent être protégés par des mesures de protection électroniques appropriées et/ou des contrôles d'accès physique qui restreignent l'accès uniquement aux utilisateurs autorisés. De même, les données de l'organisme (bases de données, etc.) doivent être stockées d'une manière qui limitera l'accès uniquement aux utilisateurs autorisés.

5.2 Rétention des données

Toutes les données sont conservées aussi longtemps que nécessaire pour parvenir aux fins pour lesquelles ils ont été recueillis et pour respecter les obligations légales de l'organisme. Le délai de rétention est calculé à partir de la date de la dernière mise à jour.

Exemple de calendrier de rétention	
Type de données	**Période de rétention**
Relevés bancaires	7 ans
Contrats et baux	7 ans
Procès-verbaux des réunions du CA	Permanent

5.3 Sauvegarde et restauration

La fréquence, l'étendue et la conservation des sauvegardes doivent être conformes à l'importance de l'information et au risque acceptable déterminé par responsable de la gouvernance des données. Les

activités de sauvegarde et de restauration des données doivent respecter les bonnes pratiques de gestion des données.

5.3.1 Effectuer des sauvegardes régulières : la fréquence des sauvegardes dépend du volume de données, de la fréquence de modification et de la criticité des données. Cependant, les sauvegardes doivent être effectuées régulièrement pour minimiser les pertes de données en cas de défaillance.

5.3.2 Utiliser des emplacements de sauvegarde hors site : pour garantir la sécurité des données, il est conseillé de stocker les sauvegardes sur un site différent du site principal. Cela peut aider à protéger les données contre les incendies, les inondations, les vols et d'autres incidents similaires.

5.3.3 Tester régulièrement les sauvegardes : les sauvegardes ne sont utiles que si elles peuvent être Restaurées avec succès. Il est donc essentiel de tester régulièrement les sauvegardes pour s'assurer qu'elles peuvent être restaurées en cas de besoin.

5.4 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 cloud, clés USB, etc.).
La SHLR adopte les niveaux de classification de données suivants :

5.4.1 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.

5.4.2 Données internes : Informations accessibles aux membres, consultants et sous-traitants qui ont besoin de les connaître à des fins professionnelles.

5.4.3 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.

5.5 Accès aux données

La SHLR 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.

5.5.1 Il est essentiel de mettre en place un système de contrôle d'accès pour empêcher l'accès non autorisé aux documents confidentiels. Les mesures de sécurité peuvent inclure l'utilisation de serrures, de codes d'accès et de caméras de surveillance.

5.5.2 Les documents confidentiels doivent être stockés dans un endroit sûr et sécurisé pour minimiser les risques de vol et de perte. Un lieu de stockage verrouillé et équipé d'un système d'alarme peut être un choix judicieux.

5.5.3 Il est important de limiter l'accès aux documents confidentiels uniquement aux membres qui ont besoin d'y accéder.

5.5.4 Les documents confidentiels doivent être protégés pendant le transport pour éviter tout accès non autorisé ou tout vol. Des mesures de sécurité telles que le scellage des boîtes et des sacs de transport peuvent être mises en place.

5.5.5 Les documents confidentiels doivent être détruits de manière sécurisée pour éviter tout accès non autorisé aux informations sensibles. Des méthodes telles que la déchiqueteuse de papier et le broyage sont des options à considérer.

5.6 Utilisation des données

Les contractuels et les membres 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. L'utilisation des données est classée dans les catégories suivantes :

5.6.1 Mise à jour : l'autorité de mettre à jour les données doit être accordée par le responsable de la gouvernance des données de la SHLR (ou une personne responsable désignée) aux personnes dont les tâches spécifient et exigent la responsabilité de la mise à jour des données.

5.6.2 Lecture seule : l'accès en lecture seule doit être autorisé par le responsable de la gouvernance des données de la SHLR (ou une personne responsable désignée) aux personnes dont les tâches nécessitent l'accès aux données.

5.6.3 Diffusion externe : Toute divulgation des données doit être approuvée par le responsable de la gouvernance des données de la SHLR (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.

6 Mise en application de cette politique

6.1 Échéance de septembre 2022

6.1.1 Désigner un (e) responsable de la protection des renseignements personnels à la SHLR

- Rendre public le titre et les coordonnées du responsable sur le site web de la SHLR
- Mettre en place une politique qui détaille les responsabilités de la SHLR

6.1.2 Procéder à l'inventaire des renseignements personnels recueillis et détenus par la Société d'histoire Les Rivières (SHLR) et évaluer leur sensibilité. Cet inventaire peut contenir les indications suivantes:

- Désignation de chaque fichier, les catégories de renseignements qu'il contient ainsi que les fins pour lesquelles les renseignements sont conservés;
- Provenance des renseignements versés à chaque fichier;
- Les catégories de personnes concernées par les renseignements versés à chaque fichier;
- Catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Mesures de sécurité prises pour assurer la protection des renseignements personnels.

6.1.3 Tenir un registre des incidents de confidentialité et, s'il y a lieu, aviser la Commission d'accès à l'information du Québec. Pour l'application de la présente loi 25, on entend par incident de confidentialité :

- L'accès non autorisé par la loi à un renseignement personnel
- L'utilisation non autorisée par la loi d'un renseignement personnel
- La communication non autorisée par la loi à un renseignement personnel
- La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

6,2 <u>Échéance de septembre 2023</u>

6.2.1 Créer ou mettre à jour une politique de confidentialité concernant les renseignements personnels obtenus par la SHLR. Cette politique doit inclure :

- Coordonnées du responsable de la protection des renseignements personnels à la SHLR
- Liste des renseignements personnels collectés par la SHLR
- Explication de l'utilisation prévue avec ces renseignements personnels
- Délai de conservation de ces données par la SHLR
- Conditions d'accès, de rectification et de retrait

6.2.2 Réviser les formulaires et contrats qui impliquent la communication de renseignements personnels aux fournisseurs de services de la SHLR.

6.2.3 Adapter tout formulaire ou contrat de service professionnel aux fins de l'obtention d'un consentement valable de la part du membre de la SHLR ou du contractuel.

6.1.4 Mettre en place des procédures ou pratiques pour le cycle de vie des données recueillies

Cette politique doit être respectée par tous les membres et contractuels de la SHLR. La vérification de la conformité à cette politique est la responsabilité du responsable de la gouvernance des données de la SHLR. 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.

Politique présentée et adoptée à Québec lors de la réunion du 5 septembre 2023 du conseil d'administration de la Société d'histoire Les Rivières (SHLR)