Société de transport du Saguenay

Politique de gestion des incidents de confidentialité

19/09/2022

1. OBJECTIF

La présente politique a pour objectif d'établir la procédure à suivre lorsque survient un incident de confidentialité au sein de la Société de transport du Saguenay (la « **S.T.S.** »). Elle prévoit également les différents éléments que la S.T.S. doit prendre en compte lorsqu'elle procède à l'évaluation d'un risque de préjudice ainsi que pour déterminer si ce préjudice est sérieux ou pas. Finalement, elle précise le contenu obligatoire du Registre des incidents de confidentialité (le « **Registre** »).

2. DÉFINITIONS

Dans la présente politique, les mots ou expressions suivant(e)s, sauf en cas d'incompatibilité, signifient ou désignent :

Incident de confidentialité **:** Accès, utilisation ou communication non autorisé par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection[1].

Préjudice sérieux **:** Acte ou événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.

Renseignement personnel **:** Information qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

3. RESPONSABILITÉS

3.1. Responsable de l'accès aux documents et de la protection des renseignements personnels

Le Responsable de l'accès aux documents et de la protection des renseignements personnels (le « **Responsable** ») veille, de manière générale, au respect et à la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignement personnels*. À ce titre, il s'assure de la mise en œuvre, de l'application et de la mise à jour de la présente politique.

[1] Article 63.9 de la *Loi sur l'accès aux documents des organismes publics et à la protection des renseignements personnels*, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*.

Il est également responsable de la tenue du Registre et doit tenir le Comité de l'accès à l'information et la protection des renseignements personnels (le « **CAIRP** ») informé des incidents qui y sont consignés.

3.2. Comité de l'accès à l'information et la protection des renseignements personnels

Le CAIRP, quant à lui, est chargé de soutenir la S.T.S., et donc le Responsable, dans l'exercice des responsabilités et dans l'exécution des obligations qui lui incombent en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignement personnels*.

À cet égard, le CAIRP peut être appelé à examiner les incidents de confidentialité et à formuler des recommandations quant aux mesures à prendre afin d'éviter que de tels incidents se reproduisent. Le CAIRP est également responsable du plan de communication, et ce, tant à l'interne qu'à l'externe. Ainsi, lorsqu'il y a un incident de confidentialité, le CAIRP est responsable :

- D'aviser les membres du personnel de la S.T.S. en leur précisant de garder l'information confidentielle;
- D'aviser la Commission d'accès à l'information et la ou les personne(s) concernée(s) par l'incident, le cas échéant;
- D'aviser tout autre personne ou organisme pertinent, s'il y a lieu.

4. PROCÉDURE À SUIVRE

4.1. Signalement

Si un membre du personnel de la S.T.S. a des raisons de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'elle détient s'est produit, il doit aviser promptement son superviseur immédiat et lui fournir toute information pertinente. Ce dernier veillera à informer le Responsable.

4.2. Évaluer la situation

Dès que le Responsable est informé du signalement, il doit notamment :

a) Aviser les intervenants concernés à l'interne, soit :

- Le CAIRP;
- Le département des technologies de l'information;
- La haute direction et, selon la gravité de l'incident, le conseil d'administration de la S.T.S..

Le Responsable doit ensuite, en collaboration avec les intervenants susmentionnés :

b) Établir les circonstances de l'incident :

- De quel type d'incident s'agit-il (accès non autorisé, utilisation non autorisée, communication non autorisée, perte ou vol de renseignements personnels, etc.) ?
- Quelle est la cause de l'incident (erreur humaine, faille ou vulnérabilité informatique, etc.) ?
- Quelle est la date ou la période visée par l'incident ?

c) Identifier les renseignements personnels impliqués[2] et leur support (papier, électronique, etc.);

d) Identifier les personnes concernées, leur nombre ainsi que leur groupe (clients, usagers, employés, etc.);

e) Répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident.

Cette évaluation doit se poursuivre tant que tous les éléments de l'incident n'ont pas été identifiés. Ensuite, ces éléments doivent être colligés dans un dossier afin de faciliter l'inscription de l'incident au Registre et l'envoi des avis, les cas échéant (voir les articles 4.5 et 4.6 de la présente politique).

4.3. Diminuer les risques

Le Responsable, en collaboration avec tout autre intervenant, doit rapidement prendre les mesures raisonnables qui s'imposent afin de

[2] Par exemple, des renseignements nominatifs, des coordonnées, des renseignements démographiques, des numéros d'assurance sociale, maladie ou du permis de conduire, des codes d'utilisateur ou mots de passe, des renseignements financiers ou médicaux, etc.

diminuer les risques qu'un préjudice soit causé, qu'il soit sérieux ou non, et afin d'éviter que de nouveaux incidents de même nature ne surviennent. Par exemple :

a) Récupérer ou exiger la destruction des renseignements personnels impliqués;

b) Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;

c) Cesser la pratique non autorisée ou non conforme;

d) Corriger les lacunes des systèmes de sécurité informatiques, etc.

4.4. Identifier la nature du préjudice

Le Responsable, en collaboration avec tout autre intervenant, doit procéder à une évaluation afin de déterminer s'il y a un risque qu'un préjudice soit causé aux personnes dont les renseignements personnels sont concernés par l'incident. L'objectif consiste à décider s'il faut aviser la Commission d'accès à l'information et les personnes concernées (voir l'article 4.5 de la présente politique).

À cet égard, plusieurs facteurs doivent être considérés afin d'identifier la nature du préjudice causé par l'incident, dont :

- La sensibilité des renseignements personnels, tels :
    - Un renseignement d'identification (numéro d'assurance sociale, d'assurance maladie, de permis de conduire, etc.);
    - Un renseignement de nature financière (numéro de carte de crédit, de compte, de transit, salaire, conditions d'emploi, etc.);
    - Un renseignement de nature médicale;
    - Un renseignement sur les origines ethniques, l'orientation sexuelle ou l'identité de genre;
    - Un renseignement génétique ou biométrique, etc.
- Les conséquences appréhendées de l'utilisation de ces renseignements, comme :

- Un vol d'identité;
- Une fraude financière ou un impact sur le dossier de crédit;
- Une diffusion des renseignements personnels, qu'ils soient sensibles[3] ou non;
- La permanence ou la perpétuité de l'atteinte;
- Une répercussion sur la santé physique ou psychologique;
- Une perte d'emploi;
- Un impact sur les relations professionnelles ou d'affaires;
- Une humiliation ou une atteinte importante à la réputation ou à la vie privée, etc.

- La probabilité que ces renseignements puissent être utilisés à des fins préjudiciables.

Le préjudice sera **sérieux** s'il est susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière **non négligeable**.

4.5. Présence d'un risque de préjudice sérieux

S'il y a un risque qu'un préjudice sérieux soit causé à la personne concernée par l'incident, le CAIRP doit **obligatoirement** :

a) Aviser la Commission d'accès à l'information dès que possible, même si toutes les informations relatives à l'incident n'ont pas encore été colligées (voir l'article 4.2 de la présente politique).

L'avis doit être fait par écrit et contenir les renseignements suivants[4] :

[3] Un renseignement personnel est considéré comme sensible lorsque, par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de respect de la vie privée.
[4] *Règlement sur les incidents de confidentialité* (projet), (2022), 26 G.O. II, 3935, art. 3.

- Le nom de l’organisation ayant fait l’objet de l’incident de confidentialité (la S.T.S.);

- Le nom et les coordonnées de la personne à contacter au sein de la S.T.S. relativement à l’incident;

- Une description des renseignements personnels visés par l’incident, ou la raison justifiant l’impossibilité de fournir une telle description;

- Une brève description des circonstances de l’incident et sa cause, si elle est connue;

- La date ou la période où l’incident a eu lieu, ou une approximation de celle-ci;

- La date ou la période au cours de laquelle la S.T.S. a pris connaissance de l’incident;

- Le nombre de personnes concernées par l’incident et, parmi celles-ci, le nombre de personnes qui résident au Québec, ou une approximation de ces nombres;

- Une description des éléments qui amènent la S.T.S. à conclure qu’il existe un risque qu’un préjudice sérieux soit causé aux personnes concernées;

- Les mesures prises par la S.T.S. ou qu’elle entend prendre afin d’aviser les personnes dont un renseignement personnel est concerné par l’incident, de même que la date où les personnes ont été avisés ou le délai d’exécution envisagé;

- Les mesures prises par la S.T.S. ou qu’elle entend prendre à la suite de la survenance de l’incident, notamment celles visant à diminuer les risques qu’un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d’exécution envisagé;

- Le cas échéant, une mention précisant qu’une personne ou un organisme situé à l’extérieur du Québec et exerçant des

responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

b) Aviser toute personne dont un renseignement personnel est concerné par l'incident, à moins que cet avis ne soit susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. L'avis doit contenir les renseignements suivants[5] :

- Une description des renseignements personnels visés par l'incident, ou la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou une approximation de celle-ci;
- Une brève description des mesures prises par la S.T.S. ou qu'elle entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
- Les mesures que la S.T.S. suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- Les coordonnées de la personne à contacter au sein de la S.T.S. afin de permettre à la personne concernée de se renseigner davantage relativement à l'incident.

Cet avis pourra être donné au moyen d'un **avis public** si le fait de le transmettre directement à la personne concernée est susceptible de causer un préjudice accru à la personne concernée, de représenter une difficulté excessive pour la S.T.S. ou lorsque la S.T.S. ne détient pas les coordonnées de la personne concernée[6].

[5] *Règlement sur les incidents de confidentialité* (projet), (2022), 26 G.O. II, 3935, art. 5.
[6] *Règlement sur les incidents de confidentialité* (projet), (2022), 26 G.O. II, 3935, art. 6.

La S.T.S. **peut** aussi aviser toute personne ou tout organisme susceptible de diminuer ce risque. Cependant, elle peut uniquement lui communiquer les renseignements personnels qui sont nécessaires à la poursuite de cet objectif. Cette communication peut se faire sans le consentement de la personne concernée, mais le Responsable doit enregistrer cette communication dans le registre approprié[7] pour garder des traces documentaires de celle-ci, comme :

- À qui ces renseignements sont communiqués;
- Dans quelles circonstances;
- Quels renseignements ont été transmis;
- Quels sont les objectifs de cette démarche, etc.

4.6. Inscrire l'incident dans le Registre

Le Responsable doit tenir un registre qui contient l'ensemble des incidents de confidentialité dont a été l'objet la S.T.S., et ce, peu importe que le risque de préjudice pour la personne concernée ait été qualifié de sérieux ou pas. Les renseignements qui s'y retrouvent doivent être conservés pour une période minimale de **cinq (5) ans** à compter de la date du premier signalement de l'incident.

Le Registre doit contenir les renseignements suivants[8] :

- Une description des renseignements personnels visés par l'incident;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu;
- La date ou la période au cours de laquelle la S.T.S. a pris connaissance de l'incident;

[7] Article 67.3 de la *Loi sur l'accès aux documents des organismes publics et de la protection des renseignements personnels*, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.*
[8] *Règlement sur les incidents de confidentialité* (projet), (2022), 26 G.O. II, 3935, art. 7.

- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;

- Une description des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque de préjudice sérieux aux personnes concernées;

- Si l'incident présente un risque de préjudice sérieux, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées de même qu'une mention indiquant si des avis publics ont été donnés par la S.T.S. et la raison pour laquelle ils l'ont été, le cas échéant;

- Une brève description des mesures prises par la S.T.S. à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

4.7. Évaluation approfondie de la situation et prévention

Lorsque toutes les étapes précédentes ont été complétées et afin d'éviter qu'un incident similaire se reproduise, le Responsable, en collaboration avec tout intervenant, doit effectuer un suivi des circonstances et des mesures prises aux étapes précédentes pour y apporter les améliorations nécessaires, le cas échéant. Ainsi, le Responsable pourrait, par exemple :

- Approfondir l'analyse des circonstances de l'incident de confidentialité et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;

- Répertorier et examiner les normes, guides, politiques ou directives internes en place au moment de l'incident, tant au niveau de la sécurité informatique qu'au niveau de la protection des renseignements personnels en général;

- Vérifier si ces normes, guides, politiques ou directives internes ont été suivies par les personnes impliquées ou identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;

- S’il s’agit d’une erreur de procédure ou d’une défaillance opérationnelle, les consigner au dossier de l’incident et adapter les processus pour éviter qu’un tel incident ne se reproduise;

- Formuler des recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;

- S’assurer de la réelle nécessité, au sein de la S.T.S., de la collecte des renseignements personnels concernés par l’incident;

- Élaborer des formations et/ou des campagnes de sensibilisation sur la protection des renseignements personnels pour les membres du personnel de la S.T.S..

5. RÉFÉRENCES

- *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1)

- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (L.Q. 2021, c. 25)

- *Règlement sur les incidents de confidentialité* (projet), (2022), 26 G.O. II, 3935

ANNEXE 1

REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Numéro de dossier à l'interne	Description des renseignements personnels visés par l'incident	Description des circonstances de l'incident	Date ou période de l'incident	Date ou période où la S.T.S. a pris connaissance de l'incident	Nombre de personne(s) concernée(s) par l'incident	Risque de préjudice sérieux? Si oui, justifiez.	Date de l'avis à la CAI (le cas échéant)	Date de l'avis à la personne concernée (le cas échéant) Avis public? Si oui, justifiez.	Mesures de protection / de mitigation prises	Mesures déployées afin qu'un tel incident ne se reproduise pas	Commentaires

Annexe 2

SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL

(articles 63.8 à 63.11 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LAI))

Les éléments illustrés ci-contre peuvent être réalisés simultanément

Motif de croire que s'est produit **un incident de confidentialité** (article 63.8 de la LAI)

Établir les circonstances de l'incident, cibler les renseignements personnels, les personnes visées et le problème

Diminuer les risques qu'un préjudice soit causé ou se reproduise (mesures de mitigation immédiates)

Déterminer la nature du préjudice en collaboration avec la personne responsable de la protection des renseignements personnels

Prendre en compte, notamment :

- la sensibilité du renseignement
- les conséquences appréhendées
- la probabilité de l'utilisation à des fins préjudiciables

(article 63.10 de la LAI)

Absence d'un risque de préjudice sérieux

Risque qu'un **préjudice sérieux** soit causé

Aviser (article 63.8 de la LAI)

Obligation
Commission d'accès à l'information

Obligation
Personnes concernées

Discrétion
Personne ou organisme susceptible de diminuer le préjudice (communication des renseignements nécessaires)

Exception
Tant que l'avis est susceptible d'entraver une enquête*
(article 63.8, alinéa 3 de la LAI)

Inscrire la communication dans un registre (responsable de la protection des renseignements personnels) (article 63.8, alinéa 2 de la LAI)

Autres mesures de mitigation afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise

Inscription de l'incident de confidentialité au registre (article 63.11 de la LAI)

Réviser le processus en continu

* Enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Québec