Politique de confidentialité et de protection de l'information

Sogi Informatique Ltée et IsoVision (ci-après « l'Organisation ») accordent une grande importance à la protection de la vie privée et des renseignements personnels et informations confidentielles qu'elles recueillent, que ce soit via leur site Web ou par tout autre moyen utilisé dans le cadre de leurs activités, quel qu'en soit le support ou la provenance.

La présente Politique décrit la manière dont l'Organisation protège les renseignements personnels qu'elle détient, en conformité avec les lois et règlements applicables en matière de protection des données, notamment la **Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)**.

En plus des renseignements personnels visés par la (LPRPSP), l'Organisation reconnaît l'existence d'informations confidentielles d'affaires qu'elle détient ou auxquelles elle a accès dans le cadre de ses activités. Ces informations ne constituent pas des renseignements personnels au sens juridique, mais méritent une protection équivalente en raison de leur nature sensible et de leur valeur commerciale, stratégique ou opérationnelle.

Définitions

- **CAI** : La *Commission d'accès à l'information du Québec* est l'organisme administratif responsable de l'application des lois en matière d'accès à l'information et de protection des renseignements personnels.
- **Incident de confidentialité** : Désigne tout accès, utilisation ou communication non autorisés, conformément à la loi, d'un renseignement personnel. Cela inclut également la perte ou toute autre atteinte à la protection d'un renseignement personnel.
- **Loi sur le secteur privé** : Fait référence à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP), chapitre P-39.1.
- **Renseignement personnel** : Tout renseignement qui concerne une personne physique et permet de l'identifier, directement ou indirectement. Par exemple : le nom, l'adresse, l'adresse courriel, le numéro de téléphone, le genre, des informations bancaires, des renseignements relatifs à la santé, l'origine ethnique, la langue, etc.
- **Renseignement personnel sensible :** Un renseignement personnel sensible est un renseignement pour lequel il existe une attente élevée en matière de protection de la vie privée. Cela inclut, par exemple, les informations de santé, les renseignements bancaires, les données biométriques, l'orientation sexuelle, l'origine ethnique, les opinions politiques, ainsi que les croyances religieuses ou philosophiques, etc.
- **Information confidentielle d'affaires**: Toute information appartenant à un client ou à un partenaire de l'Organisation, autre qu'un renseignement personnel, à laquelle l'Organisation peut avoir accès dans le cadre de ses activités, incluant notamment, sans s'y limiter : les bases de données (et leur contenu), schémas, configurations et paramètres système d'infrastructures, les informations stratégiques, commerciales ou opérationnelles, documents internes, processus, rapports, tous contenus hébergés dans les solutions de l'Organisation (ex. IsoVision), et toute

autre information d'affaires marquée « confidentielle » ou dont la nature laisse raisonnablement entendre qu'elle est confidentielle.

- **Coordonnées professionnelles ou d'affaires :** De manière générale, les coordonnées professionnelles ou d'affaires ne sont pas considérées comme des renseignements personnels. Cela inclut le nom, le titre, l'adresse, l'adresse courriel ou le numéro de téléphone d'une personne dans le cadre de son travail.

Précisions légales : Conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé du Québec* (LPRPSP), et à compter du 22 septembre 2023, les dispositions concernant la collecte, la conservation, la destruction des renseignements personnels et les mesures connexes peuvent ne pas s'appliquer aux informations relatives à l'exercice d'une fonction dans une entreprise. Cela inclut notamment le nom, le titre, la fonction, ainsi que l'adresse, l'adresse courriel et le numéro de téléphone liés au lieu de travail. De plus, ces dispositions ne s'appliquent pas aux renseignements personnels qui ont un caractère publics conformément à la loi, et ce, dès l'entrée en vigueur de la présente politique.

Responsabilités

L'Organisation est responsable de la protection des renseignements personnels et informations confidentielles d'affaires qu'elle détient ou qu'elle confie à des tiers, le cas échéant. Elle s'assure que son personnel, les membres de sa direction, ainsi que les tiers autorisés respectent la confidentialité des renseignements personnels et d'affaires auxquels ils ont accès, et ce, peu importe leur support ou la forme sous laquelle ces renseignements sont disponibles.

L'Organisation a désigné une **Personne Responsable de la Protection des Renseignements Personnels (PRPRP)**, chargée de veiller à l'application des lois en matière de protection des renseignements personnels ainsi que de la présente politique. Cette personne est notamment responsable du traitement des demandes d'accès aux renseignements personnels et de garantir leur exactitude, d'initier des rectifications si nécessaire, de gérer les incidents de confidentialité, et de promouvoir les bonnes pratiques en la matière. La PRPRP approuve également les processus, procédures et protocoles liés à la gestion des données personnelles et confidentielles d'affaires, y compris la présente politique.

Protection des informations confidentielles des clients

Dans le cadre de ses activités, notamment la fourniture de ses solutions logicielles, le support technique, la maintenance et, le cas échéant, l'hébergement ou l'assistance à l'exploitation des environnements de ses clients, l'Organisation peut être amenée à accéder à des informations appartenant à ses clients qui ne constituent pas des renseignements personnels, mais qui présentent un caractère confidentiel et stratégique.

Dans ce contexte, l'Organisation applique les principes suivants :

- **Finalité limitée :** L'accès aux données du client est strictement limité à l'exécution des obligations contractuelles de l'Organisation, notamment pour assurer le support, le diagnostic, la

maintenance ou à la demande explicite du client. Ces données ne peuvent être utilisées à d'autres fins, notamment à des fins commerciales, de développement ou d'analyse interne, sans consentement explicite du client.

- **Minimisation de l'accès :** L'Organisation accède uniquement aux données nécessaires à la réalisation du mandat. Toute copie des données du client est traitée comme un actif sensible et son accès est restreint aux membres de l'équipe impliqués dans le mandat.
- **Gestion des copies temporaires :** Toute copie des données du client obtenues dans le cadre d'un mandat est transférée et stockée de manière sécurisée dans un environnement à accès contrôlé. L'accès est limité au personnel autorisé.
- **Destruction après usage :** Dès que le mandat est complété ou que les données ne sont plus requises, toute copie des données du client est détruite de manière sécurisée ou retournée au client, selon ce qui est prévu au contrat.
- **Encadrement contractuel :** L'accès aux données client est encadré par les conditions du contrat de service en vigueur, lequel prévoit les obligations de confidentialité applicables. En l'absence de clause spécifique dans le contrat, les dispositions de la présente politique s'appliquent.
- **Obligation de discrétion du personnel :** Tout employé ou sous-traitant ayant accès à des données client dans le cadre d'un mandat est soumis à une obligation de confidentialité stricte. Toute communication de ces données à des tiers non autorisés est interdite et pourrait entraîner des mesures disciplinaires ou des recours contractuels.

En tant que prestataire de services accédant aux données de ses clients pour leur compte, l'Organisation agit à titre de sous-traitant au sens de la LPRPSP. Le client demeure le responsable du traitement de ses données. L'Organisation s'engage à respecter ce rôle et à ne jamais excéder le périmètre d'accès défini par le mandat. L'Organisation applique également des principes de gestion des incidents similaires à ceux prévus pour les renseignements personnels en cas d'incident impliquant des informations confidentielles, afin de limiter les impacts et de prévenir toute récurrence.

Renseignements personnels recueillis

Conformément au principe de précaution, l'Organisation ne collecte des renseignements personnels que lorsque cela est justifié. Toutefois, pour mener à bien sa mission, elle doit recueillir divers types de renseignements personnels.

Bien que la majorité des informations recueillies concernent ses employés et les candidats à un emploi, elles peuvent également viser des clients ou, dans une moindre mesure, d'autres parties intéressées. Les renseignements sont collectés par différents moyens, notamment via les sites Web (formulaires) de l'Organisation, par des échanges en personne, par téléphone, par courrier postal ou par courriel.

L'Organisation prend les mesures nécessaires pour s'assurer que les renseignements personnels recueillis sont adéquats, pertinents, non excessifs et utilisés à des fins limitées. Les informations collectées varient en fonction du statut de la personne et de son lien avec l'Organisation. Voici, de manière non exhaustive, les types de renseignements personnels qui peuvent être collectés :

- **Client** : Nom, prénom, téléphone professionnel, adresse courriel et adresse postale professionnelles. (Sauf exception, il s'agit principalement de coordonnées professionnelles considérées comme ayant un caractère public).
- **Personne du public** : Nom, prénom, adresse IP, adresse courriel personnelle, ainsi que toutes autres coordonnées fournies pour permettre un contact, et tout renseignement nécessaire au traitement d'une demande.
- **Employé** : Nom, prénom, sexe, date de naissance, adresse courriel personnelle, numéro de téléphone personnel, adresse postale, institution bancaire, informations gouvernementales requises pour la gestion de la paie.
- **Personne candidate à un emploi** : Nom, prénom, adresse courriel personnelle, numéro de téléphone personnel, adresse postale, diplômes, relevés de notes, curriculum vitae, attestations ou références d'emploi, et expériences professionnelles antérieures.

Fins pour lesquelles les renseignements personnels sont recueillis

L'Organisation recueille, utilise, communique et conserve des renseignements personnels concernant ses clients, employés, candidats à l'emploi, visiteurs de ses plateformes et autres tierces parties, dans le but de mener à bien ses activités.

L'Organisation informe systématiquement les personnes concernées des raisons pour lesquelles leurs renseignements personnels sont collectés. Les finalités de la collecte peuvent parfois être implicites, par exemple lorsqu'elles découlent du contexte, comme lors de la soumission d'un formulaire ou dans le cadre d'un processus d'embauche.

Les renseignements personnels recueillis par l'Organisation peuvent servir aux fins suivantes :

- **Établir des relations d'affaires** dans le cadre de potentielles ententes commerciales ;
- **Assurer le bon déroulement des activités** nécessaires à la fourniture de services à ses clients, prospects et autres partenaires d'affaires ;
- **Mener à bien les mandats confiés** par ses clients ;
- **Traiter les demandes d'inscription** aux bulletins et infolettres destinés aux clients ;
- **Gérer les demandes en lien avec les données personnelles** ;
- **Optimiser l'expérience utilisateur** sur le site Web (voir la politique des cookies) ;
- **Évaluer la pertinence des candidatures** pour les postes à pourvoir ;
- **Effectuer des vérifications préalables à l'embauche** ;
- **Gérer les dossiers de formation continue** ;
- **Effectuer les paiements ou facturer les partenaires d'affaires**, selon le cas ;
- **Remplir les obligations de l'employeur** envers ses employés, notamment (sans limitation) la gestion de la paie, l'inscription aux régimes d'assurances collectives ou d'épargne, si applicable ;

- **Soutenir la mission de l'Organisation** auprès de ses clients, partenaires d'affaires et autres parties prenantes ;

L'Organisation utilise les renseignements personnels exclusivement aux fins pour lesquelles ils ont été recueillis. Si une utilisation à d'autres fins est nécessaire, l'Organisation s'engage à informer clairement la personne concernée de la nouvelle finalité, afin qu'elle puisse donner son consentement. L'Organisation sollicite donc l'accord des personnes pour toute utilisation non prévue à l'origine, sauf dans les cas où la loi le permet ou l'exige.

Il est possible que certains renseignements personnels soient utilisés pour plusieurs finalités. Par exemple, l'adresse personnelle d'un employé peut être requise à différentes occasions pour la gestion de services comme les assurances, l'épargne retraite ou le programme d'aide aux employés, ainsi que pour communiquer avec lui.

Consentement – Collecte, utilisation et communication des renseignements personnels

L'Organisation obtient généralement le consentement de la personne concernée avant de recueillir, d'utiliser ou de communiquer ses renseignements personnels à des tiers, sauf dans les situations où la loi l'autorise ou l'exige.

Le consentement peut être implicite ou explicite, et ne nécessite pas toujours d'être formalisé par écrit. Cependant, lorsque la nature des renseignements recueillis le justifie, en raison de leur sensibilité, ou lorsque la personne concernée en fait la demande, l'Organisation peut utiliser un formulaire de consentement écrit.

L'Organisation doit également obtenir le consentement de la personne concernée avant de collecter ses renseignements personnels auprès de tiers, avant de les communiquer à des tiers, ou pour toute utilisation secondaire de ces données. Toutefois, certains renseignements personnels sont considérés comme publics par la loi, tels que les coordonnées professionnelles ou d'affaires. Dans ces cas spécifiques, le consentement n'est pas requis, car ces informations ne sont pas considérées comme confidentielles.

Accès aux renseignements personnels

Au sein de l'Organisation, seuls les employés ayant un besoin légitime dans l'exercice de leurs fonctions accèdent aux renseignements personnels. L'Organisation a mis en place des pratiques et des mécanismes internes visant à ce que chaque membre du personnel n'accède qu'aux renseignements nécessaires à la réalisation des tâches qui lui sont assignées.

Droits d’accès et de rectification – Demande et traitement

Conformément aux lois en vigueur, toute personne a le droit de demander l’accès aux renseignements personnels que l'Organisation détient à son sujet, ainsi que de demander la rectification de ces informations. Pour exercer ces droits, la personne concernée doit soumettre une demande écrite à la personne responsable de la protection des renseignements personnels chez Sogi Informatique Ltée / IsoVision (voir la section « Nous joindre » ci-après).

Toute personne concernée peut soumettre une demande portant sur les points suivants :

- **Accès** à ses renseignements personnels;
- **Rectification** de ses renseignements personnels;
- **Retrait de son consentement** à l'utilisation ou à la communication de ses renseignements personnels;
- **Portabilité** de ses données;
- **Cessation de la diffusion** de ses renseignements personnels ou **désindexation** (ces droits étant prévus par la *Loi sur la protection des renseignements personnels dans le secteur privé* - LPRPSP).

L'Organisation est tenue de répondre aux demandes d'accès, de retrait de consentement ou de cessation de diffusion des renseignements personnels dans les 30 jours suivant la réception de la demande. En ce qui concerne les demandes de rectification ou de portabilité des données, l'Organisation doit accuser réception par écrit dans ce même délai de 30 jours. Si la demande ne peut être traitée dans ce délai, la personne concernée sera informée des raisons du retard, de l'état d'avancement de la demande et du délai supplémentaire nécessaire pour fournir une réponse définitive.

L'Organisation peut exiger des informations spécifiques pour vérifier l'identité de la personne et confirmer son droit d'accès aux renseignements personnels ou à la rectification de ceux-ci. Les lois applicables permettent à l'Organisation, dans certaines circonstances, de refuser l'accès à tout ou partie des renseignements personnels détenus. En cas de refus, l'Organisation fournira une justification écrite, sous réserve des restrictions légales ou réglementaires.

Possibilité de communication des renseignements personnels à l'extérieur du Québec

Dans le cadre de ses activités, l'Organisation peut être amenée à transférer des renseignements personnels en dehors du Québec. Un tel transfert ne sera effectué que si l'Organisation a évalué que les renseignements bénéficieront d'une protection adéquate. Cette évaluation tiendra compte de la sensibilité des renseignements, de la finalité de leur utilisation et des mesures de protection en place dans la juridiction de destination. Le transfert sera également encadré par des ententes contractuelles appropriées afin de garantir que la protection des renseignements personnels est conforme aux normes en vigueur.

Mesures pour assurer la confidentialité et la sécurité des renseignements

L'Organisation met en place des mesures de sécurité appropriées (physiques, techniques et administratives) afin de protéger les renseignements personnels et les informations confidentielles contre tout accès, utilisation ou communication non autorisés, ainsi que contre toute perte ou autre atteinte à leur protection. Ces mesures sont adaptées à la nature des renseignements et visent à assurer leur confidentialité et leur intégrité.

Bien que l'Organisation applique des mesures de sécurité rigoureuses dans le cadre de son programme de **Gestion de la Cybersécurité** pour limiter les risques de violation, il subsiste un risque minime qu'une atteinte à la confidentialité ou à l'intégrité des renseignements puisse se produire en cas de faille de sécurité. L'Organisation invite toute personne ayant des raisons de croire que ses renseignements personnels ont été compromis à nous contacter dans les plus brefs délais (voir la section « Nous joindre » ci-après).

Fichiers témoins (cookies)

Un fichier témoin (ou cookie) est un petit fichier texte enregistré sur le disque dur de l'ordinateur ou d'un autre appareil de l'utilisateur. Ce fichier est entièrement inoffensif et ne peut contenir de virus.

L'Organisation a mis en place une **Politique des cookies** pour son site Web (et disponible sur celui-ci). L'objectif des fichiers témoins est d'améliorer les performances du site Web et d'enrichir l'expérience des visiteurs.

Conservation et destruction des renseignements personnels

L'Organisation conserve les renseignements personnels de manière sécurisée et ce, uniquement pour la durée nécessaire à l'accomplissement de ses obligations.

Dans de nombreux cas, les renseignements personnels seront conservés pendant plusieurs années, voire plusieurs décennies. Par exemple, les dossiers disciplinaires, d'équité salariale, de retraite, d'accidents de travail ou d'invalidité doivent être conservés suffisamment longtemps pour garantir qu'aucun droit ne soit perdu, notamment en cas de versements rétroactifs intervenant plusieurs années plus tard. Sur demande, l'Organisation fournira des explications sur la durée de conservation des renseignements personnels.

Lorsque la conservation de renseignements personnels n'est plus pertinente, l'Organisation les détruira de manière sécurisée. Toutefois, elle peut également choisir d'anonymiser les données en retirant toute information permettant d'identifier une personne, si elle souhaite conserver certains éléments pour d'autres usages.

Incidents de confidentialité et registre

L'Organisation tient un registre des incidents de confidentialité conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé* et à ses règlements. Sur demande de la **CAI** (Commission d'accès à l'information), une copie de ce registre peut lui être transmise.

Si suite à une demande ou pour toute autre raison, l'Organisation a des motifs de croire qu'un incident de confidentialité impliquant des renseignements personnels qu'elle détient s'est produit, elle doit prendre les mesures raisonnables pour réduire les risques de préjudice et éviter que des incidents similaires ne se reproduisent. Si l'incident présente un risque sérieux de préjudice, l'Organisation doit alors en informer la CAI ainsi que la personne concernée, conformément à la Loi sur le secteur privé et ses règlements.

L'Organisation applique des principes similaires en cas d'incident impliquant des informations confidentielles de clients et en informe le client dans les meilleurs délais, même si l'incident ne vise pas de renseignements personnels au sens strict de la LPRPSP. L'Organisation documente également cet incident dans son registre interne des incidents de confidentialité.

À titre de précision, un **incident de confidentialité** se définit comme :

- Un accès non autorisé par la loi à un renseignement personnel;
- Une utilisation ou une communication non autorisée par la loi d'un renseignement personnel;

- La perte de renseignements personnels ou toute autre atteinte à leur protection.

Traitement des plaintes relatives à la protection des renseignements personnels

Toute personne insatisfaite de la manière dont l'Organisation a traité ses renseignements personnels peut déposer une plainte à cet égard (voir la section « Nous Joindre » ci-après). La plainte sera examinée par la personne responsable de la protection des renseignements personnels, qui s'assurera que le traitement des renseignements est conforme aux politiques, protocoles et pratiques de l'Organisation, ainsi qu'à toute loi applicable. Toutes les communications relatives à la plainte, y compris celles par courrier ou via le formulaire en ligne, sont traitées de manière confidentielle et sécurisée pour protéger les renseignements personnels.

Si la plainte n'est pas suffisamment précise, la personne responsable de la protection des renseignements personnels peut demander des informations supplémentaires jugées nécessaires pour évaluer pleinement la plainte.

La personne ayant déposé la plainte recevra une réponse écrite par courriel dans un délai de 30 jours suivant la réception de la plainte, ou de tous les renseignements supplémentaires demandés. Si la plainte ne peut être résolue dans ce délai, le plaignant sera informé des raisons de l'extension du délai, de l'état d'avancement du traitement de la plainte et du délai supplémentaire nécessaire pour fournir une réponse définitive.

Advenant le cas ou la personne ayant déposé la plainte n'est pas satisfaite de la résolution proposée par l'Organisation, elle peut escalader la plainte auprès de l'autorité de régulation compétente, nommément la Commission d'Accès à l'information du Québec (CAI).

Nous joindre

Toute personne souhaitant contacter l'Organisation au sujet de la présente Politique, soumettre des commentaires, exercer ses droits ou déposer une plainte, est priée de remplir le formulaire ci-joint (voir à la page suivante) et le transmettre par la poste à l'adresse suivante :

Responsable de la Protection des Renseignements Personnels
Matthieu Héroux
Sogi Informatique Ltée / IsoVision
3550 Boul Gene-H.-Kruger
Trois-Rivières, Québec, Canada G9A 4M3

Historique et versions de la politique

La présente version de la Politique de confidentialité et protection de l'information (V4.0.0) est en vigueur depuis octobre 2026. Il est de la responsabilité des utilisateurs de consulter régulièrement le site Web ainsi que cette Politique afin de se tenir informés des éventuelles modifications qui pourraient y être apportées.

Formulaire de Demande concernant vos renseignements personnels

Utilisez ce formulaire pour toute demande ou plainte concernant les renseignements personnels que nous possédons à votre sujet, les modifier, les faire supprimer ou encore pour nous demander de cesser de les utiliser. Pour l'utilisation des témoins (Cookies) sur notre site Web, vous pouvez vous-même gérer vos préférences.

Important : Ne donnez aucune information confidentielle dans ce formulaire (No de passeport, carte de crédit, date de naissance, etc.). Nous vous contacterons si nous avons besoin de plus d'information.

Quel est votre lien avec Sogi Informatique Ltée / IsoVision

- ☐ Candidat(e) à un emploi
- ☐ Employé(e)
- ☐ Client ou Fournisseur
- ☐ Autre
- ☐ Visiteur du site web

Précisez :_____

Que souhaitez-vous que nous fassions au sujet de vos renseignements personnels? *(Cocher 1 seule option) :*

- ☐ Demande d'accès aux renseignements personnels que nous possédons
- ☐ Rectifier (mettre à jour) les renseignements que nous possédons
- ☐ Retirer vos coordonnées de nos listes d'envoi (publipostage, courriels etc.)
- ☐ Supprimer vos renseignements de nos dossiers
- ☐ Retirer vos coordonnées de nos listes d'envoi (publipostage, courriels etc.) **ET** Supprimer vos renseignements de nos dossiers
- ☐ Obtenir une copie des renseignements personnels informatisés que nous possédons (dans un format technologique structuré et couramment utilisé « droit à la portabilité » - si applicable)
- ☐ Plainte concernant la gestion de vos renseignements personnels
- ☐ Autre – Précisez : _____

Note : Les champs identifiés par un astérisque (*) sont obligatoires afin que nous traitions votre demande :

Prénom* _____ Nom* _____

Courriel* _____

Adresse _____

App. (facultatif) _____ Ville _____

Province / État _____ Code postal _____

Téléphone* (Ind. Régional) _____ Pays _____

SVP précisez votre demande pour nous aider à y répondre (*au besoin complétez au verso*).

Identifiant unique*: _____

(Inscrivez une courte phrase ou un identifiant alphanumérique que vous seul connaissez et gardez-en une copie. Nous vous demanderons cet identifiant lorsque nous vous contacterons au moment de traiter votre demande afin de nous assurer que c'est bien à vous que nous parlons).

☐ ***Je confirme que les informations fournies sont exactes et complètes.***

☐ ***J'accepte que les données soumises soient utilisées uniquement pour traiter ma demande.***