TECHNI CONTACT

AMX CANADA

Politique de gouvernance à l'égard de la protection des renseignements personnels

Adoptée par Julien Surprenant le 22 septembre 2023

TABLE DES MATIÈRES

PRÉAMBULE

La Politique de gouvernance à l'égard de la protection des renseignements personnels (nommée ci-après « la Politique ») est adoptée en application de la *Loi sur la protection des renseignements personnels dans le secteur privé*, c. P-39.1 (nommé ci-après «*Loi sur le privé*»).

Techni-Contact Canada Ltée et AMX Canada Ltée (nommées ci-après « Les Sociétés») sont des personne morale à but lucratif qui traitent des renseignements personnels dans le cadre de ses activités. Il est donc assujetti à la *Loi sur le privé*.

Dans le cadre de ses activités, les sociétés doivent collecter, utiliser et conserver des renseignements personnels

Cette Politique s'applique aux sociétés, ce qui inclut notamment les membres de son personnel, ses dirigeants, ainsi que toute personne qui fournit autrement des services pour le compte des sociétés.

Elle s'applique pour tous les renseignements personnels collectés, utilisés et conservés par les sociétés, et ce, peu importe leur forme. La Politique vise les renseignements personnels contenus dans tous les types de documents physiques ou numériques, au sens large, que leur forme soit écrite, graphique, sonore, visuelle, informatisée ou autre. Un renseignement personnel est défini comme étant tout renseignement qui concerne une personne physique et qui permet de l'identifier directement ou indirectement.

Les ANNEXES font partie intégrante de la Politique. Elle est remise pour lecture aux employés actuels ainsi qu'aux nouveaux membres du personnel lors de l'embauche.

1. Objectifs

La présente Politique décrit les normes de collecte, d'utilisation, de communication, de conservation et de destruction des renseignements personnels afin d'en assurer la protection. Elle explique également les rôles et les responsabilités des membres du personnel des sociétés tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ces derniers.

2. Renseignements personnels

Dans le cadre de ses activités, les sociétés peuvent recueillir et traiter différents types de renseignements personnels, notamment :

Pour le personnel :

- des renseignements d'identité, comme un nom ou un prénom, l'âge, la date de naissance, le numéro d'assurance sociale; les coordonnées bancaires pour le débit préautorisé, etc.;
- des coordonnées de contact, une adresse, une adresse électronique et un numéro de téléphone, et celles d'un tiers à contacter en cas d'urgence;
- des renseignements relatifs au processus de dotation et d'embauche, les curriculum vitae, les dossiers du personnel, les certificats de formation, les preuves de qualification, les notes d'entrevues,

- des informations contenues dans les documents d'instances connexes telles la CNESST, dossier de crédit et antécédents criminels etc.
- tout autre renseignement personnel nécessaire dans le cadre de ses activités.

3. Collecte

Les sociétés collectent des renseignements personnels principalement aux niveaux des employés actuels et futurs via son processus d'embauche.

De façon générale, les sociétés collectent les renseignements personnels directement auprès de la personne concernée et avec son consentement, sauf si une exception est prévue par la loi.

Le consentement peut être obtenu de façon implicite dans certaines situations, par exemple, lorsque la personne décide de fournir volontairement ses renseignements personnels dans le cadre d'une embauche.

Dans tous les cas, les sociétés ne collectent des renseignements personnels que s'il a une raison valable de le faire. De plus, la collecte se trouve limitée aux renseignements nécessaires dont il a besoin pour remplir l'objectif visé.

À moins d'une exception prévue par la loi, les sociétés demandent le consentement de la personne concernée avant de collecter des renseignements personnels qui la concernent auprès d'un tiers.

Considérant que les sociétés collectent des renseignements personnels par un moyen technologique, elles se sont dotées d'une Politique de confidentialité lors d'une collecte de renseignements personnels par un moyen technologique, disponible à l'**ANNEXE 1**.

4. Utilisation

Les sociétés s'engagent à utiliser les renseignements personnels en sa possession uniquement aux fins pour lesquelles ils ont été recueillis et pour lesquels la loi l'autorise à les utiliser. Il peut toutefois les recueillir, les utiliser ou les divulguer sans le consentement de la personne visée lorsque cela est permis ou exigé par la loi.

Dans certaines circonstances particulières, les sociétés peut recueillir, utiliser ou divulguer des renseignements personnels sans que la personne concernée n'en soit informée ou qu'elle n'ait donné son consentement. De telles circonstances sont réunies notamment lorsque, pour des raisons juridiques, médicales ou de sécurité, il est impossible ou peu probable d'obtenir son consentement, lorsque cette utilisation est manifestement au bénéfice de cette personne, lorsque cela est nécessaire pour prévenir ou détecter une fraude ou pour tout autre motif sérieux.

Les sociétés limitent l'accès des membres du personnel et des dirigeants aux seuls renseignements personnels et connaissances de nature personnelle qui sont nécessaires à l'exercice de leur fonction.

5. Communication

En général, les sociétés ne peuvent communiquer les renseignements personnels qu'il détient sur une personne sans le consentement de celle-ci.

Toutefois, les sociétés peuvent communiquer à un tiers des renseignements personnels sans le consentement de la personne concernée lorsqu'est prévue une exigence réglementaire ou légale ou lorsque la Loi sur le privé ou toute autre loi le permet.

6. Conservation

Conservation

Dans le cadre de ses activités, les sociétés doivent conserver de nombreux documents comportant des renseignements personnels.

Certains documents doivent être conservés pendant une durée prescrite par la *Loi sur les impôts* ou toutes autres instances qui régissent la corporation.

Qualité des renseignements personnels

Les sociétés s'assurent de la qualité des renseignements personnels qu'elles détiennent. En ce sens, les renseignements personnels conservés sont à jour, exacts et complets et servent aux fins pour lesquelles ils ont été recueillis ou utilisés.

La mise à jour constante des renseignements personnels n'est pas nécessaire, sauf si cela est justifié par les fins pour lesquelles ces renseignements sont recueillis. Cependant, si les renseignements doivent servir à une prise de décision, ils doivent être à jour à ce moment.

Documents physiques et numériques

Selon la nature des renseignements personnels, ceux-ci peuvent être conservés aux bureaux des sociétés, dans divers systèmes informatiques des sociétés, ou de ses fournisseurs de services, ou dans les installations d'entreposage des sociétés ou de ses fournisseurs de services.

Mesures de sécurité

La sécurité et la protection des renseignements personnels sont importantes pour les sociétés qui met en place des mesures de sécurité afin que les renseignements personnels demeurent strictement confidentiels et soient protégés contre la perte ou le vol et contre tout accès, communication, copie, utilisation ou modification non autorisés.

Ces mesures de sécurité peuvent comprendre notamment des mesures organisationnelles telles que l'utilisation de classeurs et d'armoires de rangement verrouillés et dont l'accès est restreint au personnel concerné et à ce qui est nécessaire, l'accès aux bureaux verrouillés, les rappels des procédures liées à la confidentialité et à la protection des renseignements personnels en réunion d'équipe, l'utilisation de procédures de sécurité et de registres variés (procédures d'embauche, registre de prise de connaissance de la Politique par le personnel, registre des incidents de confidentialité…), l'utilisation d'une déchiqueteuse ou toutes autres pratiques jugées nécessaires à la protection des données personnelles. Pour les pratiques concernant la protection des renseignements informatisés, consulter l'Annexe 1 - Politique de confidentialité lors d'une collecte de renseignements personnels par un moyen technologique.

7. Destruction

La destruction des documents d'origine contenant des renseignements personnels ou confidentiels est faite de façon sécuritaire.

Les sociétés utilisent des techniques de destruction des documents adaptées au niveau de confidentialité du document à détruire.

8. Évaluation des facteurs relatifs à la vie privée

Les sociétés doivent procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) pour tout nouveaux projets impliquant la collecte et/ou l'utilisation de renseignements personnels, de développement et de refonte de systèmes d'informations ou de prestation électronique de services impliquant des renseignements personnels.

L'évaluation des facteurs relatifs à la vie privée réalisée doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

Les sociétés peuvent s'aider du guide développé par la Commission d'accès à l'information « Guide d'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée » pour réaliser l'évaluation des facteurs relatifs à la vie privée, le cas échant.

9. Demande d'accès ou de rectification

Toute personne peut faire une demande d'accès ou de rectification concernant les renseignements personnels détenus par les sociétés. Sous réserve de certaines restrictions légales, les personnes concernées peuvent demander l'accès à leurs renseignements personnels détenus par les sociétés et en demander leur correction dans le cas où ils sont inexacts, incomplets ou équivoques

Pour des corrections, vous adresser au Responsable de la protection des renseignements personnels des sociétés qui répond par écrit à ces demandes dans les 30 jours de la date de réception.

10. Incidents de confidentialité

Les incidents de confidentialité

Un incident de confidentialité correspond à un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

Lorsqu'il a des motifs de croire qu'il s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, les sociétés prennent les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

En cas d'incident de confidentialité, les sociétés procèdent à l'évaluation du préjudice. Cette évaluation tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Quand l'incident présente le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, les sociétés avisent par écrit :

- La Commission d'accès à l'information via le formulaire d'avis prescrit ;
- La ou les personnes concernées. L'avis doit permettre de la renseigner adéquatement sur la portée et les conséquences de l'incident.
- Cet avis doit contenir :
    - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
    - Une brève description des circonstances de l'incident;
    - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
    - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident;
    - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou atténuer celui-ci;
    - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

Registre des incidents de confidentialité

Les sociétés tiennent un registre des incidents de confidentialité prévu à **l'ANNEXE 3.**

Le registre collige l'ensemble des incidents de confidentialité impliquant un renseignement personnel, ceux présentant un risque de préjudice sérieux comme ceux ne présentant pas de risque de préjudice sérieux.

Les renseignements contenus au registre des incidents de confidentialité sont tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle les sociétés ont pris connaissance de l'incident.

11. Processus de traitement des plaintes en lien avec la protection des renseignements personnels

Toute personne concernée par l'application de la présente Politique peut porter plainte concernant son application ou, plus généralement, concernant la protection de ses renseignements personnels par les sociétés.

La procédure de traitement de plainte relative à la protection des renseignements personnels est prévue à **l'ANNEXE 4.**

12. Coordonnées de la responsable de la protection des renseignements personnels

Julien Surprenant, Responsable de la protection des renseignements personnels des Sociétés, peut être jointe par téléphone au 514-695-4883 poste 232. Il est possible de communiquer avec lui pour toute question en lien avec l'application de la présente Politique.

13. Entrée en vigueur de la politique

La Politique entre en vigueur le 23 septembre 2023.

La Politique a été approuvée par la Responsable de la protection des renseignements personnels.

S'ils modifient la présente Politique, les sociétés rendent disponible la Politique tel que modifiée.

ANNEXE 1 – POLITIQUE DE CONFIDENTIALITÉ LORS D'UNE COLLECTE DE RENSEIGNEMENTS PERSONNELS PAR UN MOYEN TECHNOLOGIQUE

Les sociétés s'engagent à assurer la protection et la confidentialité des renseignements personnels que vous fournissez ou que nous recueillons lorsque vous interagissez avec nous par moyen technologique. À cet égard, la présente politique de confidentialité (ci-après la « Politique ») vise à vous informer des renseignements personnels collectés, des fins pour lesquelles ceux-ci sont recueillis, des communications qui pourraient être effectuées et, de manière générale, des mesures de protection mises en place.

La Politique de confidentialité est adoptée en application de l'article 8.2 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, c. P-39.1 (ci-après « *Loi sur le privé* »).

Consentement

En dehors des renseignements personnels exigés par la loi, la décision de nous fournir ou non vos renseignements personnels vous revient exclusivement. En règle générale, vous pouvez communiquer avec nous sans avoir à nous les fournir.

Si vous utilisez nos services ou si vous soumettez vos renseignements personnels aux sociétés, vous serez réputé avoir donné votre consentement aux fins énoncées ci-après, pour lesquelles les sociétés recueillent et utilisent vos renseignements personnels.

Partage et communication de l'information

Généralement, les sociétés ne peuvent transmettre vos renseignements personnels à d'autres organisations sans votre consentement. Nous pourrions communiquer vos renseignements personnels sans votre consentement si la loi nous y oblige ou le permet, mais, le cas échéant, nous ne fournirons que les renseignements qui sont exigés.

Stockage et sécurité

Tous les renseignements personnels que vous fournissez aux sociétés sont sauvegardés et archivés sur des serveurs sécurisés, à accès restreint des sociétés. Par ailleurs, en partenariat avec le consultant externe Exosource, les sociétés prennent des moyens techniques variés pour assurer un environnement sécuritaire et pour protéger vos renseignements personnels, notamment en utilisant des barrières coupe-feu et des antivirus, en gérant les accès, en utilisant des procédés d'authentification multi-facteur (AMF), en utilisant le verrouillage automatique, en effectuant des copies de sauvegarde régulières, en utilisant des mots de passe sécurisés, en utilisant un système de partage de documents sécurisé et en suivant des procédures strictes. Par ailleurs, les sociétés travaillent de façon continue en collaboration avec son consultant en informatique dans le but d'optimiser et de parfaire ses mécanismes de sécurité.

Cependant, étant donné la nature même du réseau public qu'est l'internet, vous reconnaissez et acceptez que la sécurité des transmissions via internet ne puisse être garantie. En conséquence, les sociétés ne peuvent garantir ni assumer aucune responsabilité pour toute violation de confidentialité, piratage, virus, perte ou altération des données transmises par Internet.

Numérisation des documents

Les sociétés choisit un support ou une technologie sur lequel il conserve ses documents ainsi que des procédures qui lui permettent de respecter les conditions suivantes :

1. L'information contenue dans les documents numérisés n'a pas été altérée et elle a été maintenue dans son intégralité ;
2. La numérisation ainsi que le support pour conserver les documents numérisés doit assurer la stabilité et la pérennité des documents.

Lorsque les sociétés effectuent une numérisation, elles appliquent les procédures prévues à l'**ANNEXE 2.**

Conservation

Les sociétés utilisent et conservent vos renseignements personnels aussi longtemps que nécessaire afin de satisfaire les finalités pour lesquelles ils ont été recueillis, ou comme la loi le permet ou l'exige.

Les sociétés se réservent le droit de détenir, pour une durée raisonnable, certains renseignements personnels pour se conformer à la loi, prévenir la fraude, résoudre une réclamation ou certains autres problèmes s'y rattachant, coopérer à une enquête et pour tout autre acte permis par la loi. À l'expiration de ce délai, vos renseignements personnels sont délestés des serveurs des sociétés.

Liens externes

La présente Politique ne s'applique pas aux sites internet de tiers auxquels il est possible d'accéder en cliquant sur des liens et les sociétés ne sont nullement responsables à l'égard des sites Internet de tiers. Les sociétés ne font aucune représentation concernant tout autre site auquel vous pourriez avoir accès à partir de nos communications. Si vous suivez un lien vers un site Web de tiers, celui-ci disposera de ses propres politiques sur la protection des renseignements personnels que vous devrez examiner avant de soumettre les renseignements personnels demandés.

De plus, un lien vers un tel site ne signifie pas que les sociétés recommandent ce site tiers ou qu'elle assume une quelconque responsabilité quant à son contenu ou à l'usage qui peut en être fait. Il vous incombe de prendre les précautions nécessaires pour vous assurer que le site que vous sélectionnez pour votre usage n'est pas infecté de virus ou d'autres parasites de nature destructrice.

Informations additionnelles

Pour toute demande d'information ou mise à jour concernant vos renseignements personnels, veuillez joindre par téléphone Julien Surprenant, Responsable de la protection des renseignements personnels, au 514-695-4883 poste 232.

Modification

Les sociétés se réservent le droit de modifier leur Politique de confidentialité à leur discrétion. Les sociétés rendront disponible toute modification éventuelle de cette Politique de confidentialité.

ANNEXE 2 – PROCÉDURE DE NUMÉRISATION

La personne responsable de la numérisation :

1. Effectue la préparation physique des documents à numériser (enlève les trombones et les agrafes);
2. Numérise les documents et demeure présente tout au long du processus afin de protéger l'intégrité des données numérisées;
3. Effectue une vérification exhaustive des documents numérisés afin de s'assurer de la quantité, de la qualité et de l'intégrité des documents reproduits. Elle vérifie que :
    - les documents numérisés sont conformes aux documents sources;
    - les données sont lisibles et de bonne qualité (sans perte de détail ou d'information);
    - le recto verso a bien été fait, le cas échéant; si l'option recto verso a fait en sorte de laisser des pages blanches, elle élimine ces dernières;
    - les documents ou les pages ont été numérisés dans le bon sens.
4. Vérifie que le nombre de documents ou de pages est exact (si des pages manquent, elle reprend la numérisation au complet);
5. Renomme les fichiers PDF selon la convention de nommage établie dans les sociétés;
6. Enregistre le ou les fichiers PDF dans le logiciel approprié des sociétés;

ANNEXE 3 – REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Registre des incidents de confidentialité								
Date ou période de l'incident	Prise de connaissance de l'incident	Nombre de personnes concernées par l'incident	Personnes concernées (informations compromises)	Description des circonstances de l'incident	Description des risques de préjudices	Date de transmission de l'avis à la Commission d'accès à l'information	Date de transmission des avis aux personnes concernées	Description des mesures prises

ANNEXE 4 – PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Réception de la plainte

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 par les sociétés, doit le faire par écrit en s'adressant à la Responsable de la protection des renseignements personnels des sociétés.

La personne devra indiquer son nom, les coordonnées pour la 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. Si la plainte formulée n'est pas suffisamment précise, la responsable de la protection des renseignements personnels peut requérir toute information additionnelle qu'elle juge nécessaire pour pouvoir évaluer la plainte.

Traitement de la plainte

Les sociétés s'engagent à traiter toute plainte reçue de façon confidentielle.

Une évaluation est effectuée pour déterminer si le traitement des renseignements personnels par les sociétés est conforme à la Politique et aux pratiques en place au sein de l'organisation et à la législation ou réglementation applicable.

La plainte est traitée dans un délai raisonnable. La Responsable de la protection des renseignements personnels doit évaluer la plainte et formuler une réponse motivée écrite à la personne plaignante.

Dossier de plainte

Les sociétés doivent constituer un dossier distinct pour chacune des plaintes qui lui sont adressées en vertu de la présente procédure de traitement de plainte. Chaque dossier contient la plainte, l'analyse et la documentation à l'appui de son évaluation, ainsi que la réponse écrite envoyée à la personne plaignante.