Politique de protection des renseignements personnels

1.1 Aperçu

La politique du Partenariat en matière de protection des renseignements personnels est fondée sur les dix principes interdépendants constituant la base du Code type de la CSA pour la protection des renseignements personnels décrits à la section 1.4.1 ci-après. Ces principes, établissant le cadre des pratiques exemplaires en matière de protection des renseignements adoptées à l'échelon fédéral, provincial et territorial, sont étroitement intégrés à l'ensemble des lois et des règlements régissant ce domaine au Canada.

Il est indispensable que les principes et les pratiques exemplaires associés à la protection des renseignements personnels soient compris de tous les utilisateurs de ce type de renseignements pour que le Partenariat soit certain de disposer d'un cadre de sécurité et de protection des renseignements personnels pleinement opérationnel. En outre, lesdits principes et lesdites pratiques exemplaires doivent être intégrés aux pratiques quotidiennes au sein de l'organisation. Pour ce faire, il convient de promouvoir une culture au sein de laquelle la protection des renseignements est considérée comme un objectif de conception des systèmes informationnels et de technologies de l'information (TI) et non comme un obstacle à surmonter. La sécurité et la protection des renseignements personnels font partie des droits fondamentaux de la personne inscrits dans les lois prévalant un peu partout dans le monde.

La présente politique fournit à l'organisation des orientations de gestion sur les mesures à prendre pour protéger les renseignements personnels administrés par le Partenariat, ou qui sont sous son contrôle, sans toutefois préciser les modalités de leur mise en œuvre que l'on trouvera exposées en détail dans d'autres composantes du Cadre de sécurité et de protection des renseignements personnels du Partenariat. Le Partenariat pourrait, à sa seule discrétion, imposer des directives supplémentaires en la matière.

1.2 But

Cette politique a pour but de définir des règles de configuration et de gestion de la confidentialité qui permettent de garantir la protection des renseignements personnels administrés par le Partenariat ou qui sont sous son contrôle :

i. Prévoir la collecte, l'utilisation, la conservation et la divulgation des renseignements personnels par le Partenariat ainsi que leur sécurité, dans le respect de la loi
ii. Renforcer la conviction du public et des partenaires quant au fait que le Partenariat applique des politiques et des pratiques exemplaires en matière de protection des renseignements personnels dans le cadre de la conception, de la mise en œuvre et de l'évolution de ses programmes, de ses systèmes et de ses services

iii. Exiger la mise en œuvre d'évaluations de la sécurité et de la protection des renseignements personnels ainsi que la prise en compte rapide de tout problème recensé par lesdites évaluations

iv. Exiger la mise en place d'ententes de partage de renseignements lorsque des renseignements personnels sont partagés avec des tiers

v. Exiger que les dossiers relatifs aux ententes de partage d'information, aux évaluations des facteurs relatifs à la vie privée et aux évaluations des risques et des menaces soient gérés de façon centralisée, en conformité avec le degré de sensibilité des renseignements concernés et les exigences d'accès

La présente politique permet au Partenariat de minimiser ses risques et de faire preuve de diligence vis-à-vis de ses partenaires, des intervenants et du grand public.

1.3 Portée

Cette politique s'applique à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat qui gèrent l'accès à des renseignements personnels stockés au sein de ses ressources TI et à qui il incombe d'en garantir la sécurité et la protection. Elle s'applique également au personnel, au conseil d'administration, aux consultants, aux sous-traitants et aux partenaires du Partenariat qui manipulent des renseignements personnels sous quelque forme que ce soit.

Afin de faciliter la compréhension et le respect de cette politique, l'ensemble des membres du personnel et du conseil d'administration du Partenariat recevra une formation de sensibilisation à la sécurité et à la protection des renseignements personnels.

1.4 Énoncé de politique

1.4.1. Principes de protection des renseignements

i. Responsabilisation

La responsabilité de la conformité du Partenariat à l'égard de cette politique incombe à son PDG, qui pourra dans la pratique, déléguer cette tâche à une personne agissant au titre de chef de la sécurité et de la protection des renseignements personnels (CSPRP).

Le Partenariat offrira à son personnel une formation en matière de sécurité et de protection des renseignements personnels afin de l'aider à mettre en œuvre les procédures d'accès et de diffusion appuyant la présente politique.

ii. Détermination des fins

Il incombera au Partenariat de déterminer, avant leur collecte ou au moment de leur collecte, les fins auxquelles des renseignements personnels sont recueillis, ces renseignements personnels ne devant alors être utilisés qu'aux fins précisées à la

personne concernée, au moment de leur collecte ou avant leur collecte, sauf si cette dernière donne son consentement pour d'autres utilisations ou d'autres divulgations.

iii. Consentement

Il incombera au Partenariat d'obtenir le consentement de la personne pour la collecte, l'utilisation et la divulgation de ses renseignements personnels, sauf dans les cas où l'absence d'un tel consentement est autorisée par la loi.

Dans ce cadre, le Partenariat utilisera un modèle de consentement implicite en toute connaissance de cause. « En toute connaissance de cause » signifie qu'une personne connaît les fins auxquelles ses renseignements personnels sont recueillis, utilisés ou divulgués et est informée qu'elle peut donner ou retirer son consentement à cette collecte, à cette utilisation ou à cette divulgation. « Implicite » signifie que ce consentement n'a pas besoin d'être explicite (un consentement est explicite lorsqu'il est par exemple communiqué verbalement ou par écrit), mais que le Partenariat peut supposer qu'il y a consentement lorsqu'il est raisonnable de le penser.

iv. Limite de la collecte

Le Partenariat limitera la collecte de renseignements personnels à ce qui est nécessaire. Lors de la conception de systèmes d'information ou de processus opérationnels, on prendra en compte la volonté de limiter les données requises.

v. Limites de l'utilisation, de la divulgation et de la conservation

Les renseignements personnels ne pourront être utilisés ou divulgués qu'aux fins pour lesquelles ils ont été recueillis, sauf avec le consentement de la personne ou en conformité avec la loi.

Tous les systèmes de stockage de renseignements devront être dotés de calendriers de conservation et d'élimination.

vi. Exactitude et intégrité

Le Partenariat sera doté de procédures permettant de veiller à l'exactitude et à l'actualité de tous les renseignements personnels conservés dans ses systèmes de stockage.

vii. Mesures de protection

Les renseignements personnels recueillis, utilisés et divulgués par le Partenariat devront être protégés par des mesures proportionnelles à leur degré de sensibilité, visant à prévenir toute utilisation, divulgation ou suppression involontaire ou non autorisée.

viii. Ouverture des politiques, des procédures et des pratiques

Le Partenariat mettra à la disposition du public des renseignements précis sur ses politiques, ses procédures et ses pratiques en matière de gestion des renseignements personnels. À la suite d'une demande en ce sens, le Partenariat pourra en outre décider, à sa seule discrétion, de communiquer des renseignements généraux associés aux

résultats des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations des menaces et des risques (EMR) qu'il aura conduites.

ix. Accès individuel

Le Partenariat mettra en œuvre des systèmes et des processus opérationnels visant à faciliter l'accès des personnes aux renseignements personnels les concernant. De la même façon, le Partenariat mettra à la disposition des personnes les moyens de contester l'exactitude et l'exhaustivité des renseignements personnels qu'il détient et d'en obtenir, s'il y a lieu, la modification.

x. Contestation de la conformité et plaintes

Pour toute question relative à sa conformité avec ses politiques et pratiques exemplaires, le Partenariat encouragera les parties concernées à communiquer avec lui en utilisant les coordonnées fournies. En cas de plainte ou de différend concernant la collecte, l'utilisation ou la divulgation de renseignements personnels considérées comme inappropriées et non conformes aux principes de protection des renseignements personnels et aux pratiques exemplaires en matière de sécurité constituant la base de son cadre de protection des renseignements, le Partenariat ouvrira une enquête et tentera de trouver une solution.

1.4.2 Évaluation des facteurs relatifs à la vie privée (EFVP)

i. On conduira une EFVP afin de déterminer si un projet, un programme, une application, un système ou une nouvelle disposition sur la façon de recueillir, d'utiliser, de conserver, de divulguer ou de sécuriser des renseignements personnels présente des risques en matière de protection des renseignements personnels.

ii. Les partenaires du Partenariat exploitant ses systèmes TI (par exemple un site fourni en « marque blanche ») devront conduire une EFVP, dont les résultats devront être validés par le Partenariat avant l'activation du service ou le lancement du programme concerné.

1.4.3 Évaluation des risques et des menaces (ERM)

i. Une ERM devra être menée pour déterminer les menaces et les vulnérabilités associées au stockage et à la gestion des renseignements au sein d'un projet, d'un programme, d'une application ou d'un système. Toute ERM menée dans ce cadre devra clairement recenser les risques susceptibles de compromettre des renseignements personnels.

1.4.4 Accords de partenariat

i. Le Partenariat élaborera, au besoin, des ententes de partage de renseignements avec des tiers dans le seul but d'assurer la sécurité et la protection des renseignements personnels échangés entre les deux parties. Il s'agira notamment des renseignements stockés dans les systèmes TI du Partenariat ou dans des systèmes de partenaires dans

d'autres provinces. Ces ententes pourront constituer des documents autonomes ou des sections au sein d'autres ententes.

ii. Le Partenariat examinera, au moins une fois par an, les sommaires des ententes de partenariat et de partage de renseignements existantes.

1.5 Contrôle de l'application de la politique

En cas de non-respect de cette politique, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

i. Refuser l'accès à ses ressources informationnelles et TI.

ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.

iii. Mettre en œuvre, pour les employés, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement, la cessation immédiate de l'emploi ou des poursuites en vertu de la loi.

1.6 Définitions

Terme	Définition
Accès	Droit d'une personne ou de son représentant autorisé à obtenir du Partenariat les renseignements personnels la concernant.
Responsabilisation	Une organisation est responsable des renseignements personnels qu'elle contrôle et doit désigner une ou plusieurs personnes responsables de sa conformité avec le Code type de la CSA pour la protection des renseignements personnels, avec ses propres politiques ainsi qu'avec les lois et règlements applicables.
Exactitude	L'enregistrement d'énoncés factuels, d'opinions, de jugements ou d'évaluations reflétant le plus fidèlement possible les éléments fournis par la personne et les éléments que l'organisation collectrice a établi, déterminé ou présumé comme étant vrais.
Consentement	La personne doit volontairement donner son accord pour la collecte, l'utilisation et la divulgation de ses renseignements personnels. Ce consentement peut être explicite ou implicite, et

	doit inclure une explication quant aux répercussions d'un retrait du consentement. Un consentement explicite est formulé de façon non ambiguë, verbalement ou par écrit. Il est sans équivoque et ne nécessite aucune inférence de la part de l'organisation l'ayant sollicité. Un consentement est implicite lorsque les agissements ou l'absence d'agissements d'une personne permettent raisonnablement de déduire qu'elle donne son consentement. Le consentement ne doit jamais être une condition pour fournir un produit ou un service, à moins que les renseignements demandés ne soient requis pour réaliser un objectif légitime et explicitement spécifié.
Contrôle des renseignements	Renseignements administrés par le Partenariat (voir la définition ci-après) recueillis, acquis, mis à jour, supprimés, utilisés et divulgués à sa discrétion et dans les limites de la loi
Administration des renseignements	Renseignements conservés ou stockés par le Partenariat dans ses bureaux, installations, meubles de rangement ou ordinateurs
Divulgation	Communication ou mise à la disposition de renseignements personnels à un tiers n'étant ni employé ni au service de l'organisation ou de la personne détentrice desdits renseignements

Renseignements personnels	Renseignements enregistrés à propos d'une personne identifiable, notamment : • Les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge, à son sexe, à son orientation sexuelle, à son statut familial ou marital. • Les renseignements relatifs à son éducation ainsi qu'à ses antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels et les renseignements relatifs aux transactions financières qu'elle a effectuées. • Tout numéro d'identification, symbole ou autre élément précis lui ayant été attribué. • Son adresse, son numéro de téléphone, ses empreintes digitales ou son type sanguin. • Ses opinions personnelles, sauf si elles concernent une autre personne. • La correspondance qu'elle a adressée au Partenariat et qui est implicitement ou explicitement de nature privée ou confidentielle, ainsi que les réponses à cette correspondance susceptible d'en révéler le contenu. • Les opinions d'une autre personne à son propos. • Son nom lorsqu'il figure conjointement avec d'autres renseignements personnels la concernant ou lorsque la divulgation de son nom permettrait de révéler d'autres renseignements personnels la concernant. On appelle renseignements identifiables toutes les données qui permettent d'établir un lien unique entre une personne et d'autres données. Il peut s'agir notamment de codes NIP (numéro d'identification personnel), de cartes d'accès, de mots de passe, d'empreintes rétiniennes et digitales ainsi que d'adresses de courriel ou d'adresses IP. Ce type de renseignements doit être traité de la même façon que des renseignements personnels recueillis dans un environnement hors ligne.
Confidentialité	Droit d'une personne à contrôler la collecte, l'utilisation et la divulgation de ses renseignements personnels.

Mesures de protection	Les renseignements personnels doivent être protégés par des mesures de sécurité proportionnelles à leur degré de sensibilité.
Utilisation	On appelle utilisation le traitement et la manipulation de renseignements personnels au sein d'une organisation.
Collecte	Processus de collecte ou d'obtention de renseignements personnels. Les renseignements peuvent être collectés directement auprès d'un client ou indirectement, par exemple lorsqu'une personne fournit une autorisation légale en ce sens à un représentant ou à un dépositaire.
Sécurité	Moyens par lesquels des renseignements ou des données sont protégés d'une divulgation, modification, suppression ou destruction accidentelle ou malveillante
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI
Cadre de sécurité et de protection des renseignements personnels	Ensemble des politiques, des normes, des outils, des gabarits, des processus et des procédures qui régissent, individuellement et collectivement, la confidentialité, la protection et la sécurité des ressources informationnelles et TI du Partenariat

Documents connexes

- Politique de gestion de l'information
- Politique de gestion des dossiers
- Politique de sécurité de l'information et des technologies de l'information

- Politique de classification des renseignements
- Politique de consultation et de diffusion des renseignements personnels
- Procédures de consultation et de diffusion des renseignements personnels
- Politique d'utilisation acceptable
- Modèle d'évaluation des facteurs relatifs à la vie privée
- Gabarit d'évaluation des risques et des menaces
- Gabarit d'entente de partage de données

Fin du document