Échange de renseignements entre entités déclarantes

Modèle de code de pratique

Avertissement

Le présent document est un **modèle** de code de pratique qui vise à **aider** les entités déclarantes en leur fournissant un exemple de ce qui pourrait être pris en compte dans l'élaboration volontaire de codes de pratique particuliers qui répondraient aux besoins de chaque entité déclarante participante en fonction de son secteur ou de cas d'utilisation qui lui sont propres.

Le présent document ne se veut qu'une directive générale. Chaque section présente des exemples de ce qui pourrait être inclus dans un code de pratique. Il incombe toutefois aux entités déclarantes de préparer et de déterminer l'information et les détails pertinents qui sont nécessaires pour répondre aux exigences d'un code de pratique.

Les codes de pratique soumis au Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) et au Commissariat à la protection de la vie privée doivent être adaptés à la réalité unique des entités déclarantes participantes. Le fait de s'inspirer du présent document ne garantit pas l'approbation du Commissariat à la protection de la vie privée. Tous les codes doivent être soumis à CANAFE aux fins d'examen et au Commissariat à la protection de la vie privée du Canada aux fins d'approbation.

Table des matières

Code de pratique

1. Application

Le présent Code de pratique s'applique à tous les participants figurant à l'annexe A du présent document. Tous les participants sont des « personnes » et des « entités » visées à l'article 5 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (la Loi).

2. Fins pour lesquelles l'on peut communiquer, collecter ou utiliser des renseignements personnels

Remarque : Il est recommandé d'énumérer des fins précises et pertinentes à votre situation particulière afin de bien mettre en contexte le Commissariat à la protection de la vie privée.

La communication, la collecte et l'utilisation de renseignements personnels par les participants au présent Code de pratique visent précisément à détecter et à décourager le blanchiment d'argent, le financement des activités terroristes et le contournement des sanctions, conformément à la Loi (comme expliqué dans la section 6 du présent Code). Les participants ne peuvent utiliser les renseignements qu'à des fins autorisées ou requises par les lois applicables.

Pour poursuivre ces fins, les renseignements personnels communiqués, collectés et utilisés dans le cadre du présent Code de pratique serviront :

- à la détection et à la perturbation d'activités illicites associées à une variété de plateformes, d'opérations et de réseaux financiers;
- à la mise en œuvre des exigences législatives et réglementaires prévues par la Loi, comme pour la déclaration d'opérations douteuses;
- à la réduction du cloisonnement de l'information et des angles morts exploités par les criminels;
- à l'accroissement de l'efficacité de l'évaluation des risques associés aux clients et de la surveillance en fonction du niveau de risque.

Aux fins du présent Code de pratique, la définition du terme « renseignement personnel » est la même que celle de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), comme cela est cité à l'annexe B.

Dès la réception des renseignements, les participants au Code sont tenus d'évaluer ce qui leur est demandé, le cas échéant. Les participants n'ont à prendre aucune mesure que ce soit à la réception des renseignements.

3. Renseignements personnels que l'on peut communiquer, collecter ou utiliser

Les renseignements personnels que l'on peut communiquer, collecter ou utiliser comprennent ceux qui ont été légalement obtenus dans le cadre des activités du participant et qui sont raisonnables aux fins de détection ou de découragement du blanchiment d'argent, du financement des activités terroristes ou du contournement des sanctions.

Les catégories ci-dessous regroupent les renseignements personnels que les participants au présent Code de pratique peuvent communiquer, collecter ou utiliser aux fins décrites précédemment :

- Renseignements collectés dans le cadre des activités d'un participant concernant toute personne ou entité pertinente. Il peut s'agir, par exemple, d'un nom, d'une adresse, d'une adresse courriel, d'un numéro de téléphone, de documents d'identité, de la citoyenneté, de l'employeur, ou du bénéficiaire effectif.

- Renseignements collectés dans le cadre des activités d'un participant sur des opérations pertinentes réalisées ou tentées. Il peut s'agir, par exemple, de la date, de l'heure et du lieu des opérations, du type et de la somme des fonds ou autres actifs concernés, ou des identifiants des opérations.

- Renseignements collectés dans le cadre des activités d'un participant relatives aux comptes. Il peut s'agir, par exemple, de titulaires de comptes, de numéros de compte, de numéros de référence, de numéros de succursales, ou de numéros d'institutions.

- Renseignements collectés dans le cadre des activités d'un participant associées à l'utilisation d'interfaces en ligne. Il peut s'agir, par exemple, de renseignements relatifs aux appareils utilisés lors des opérations, aux adresses de protocole Internet, et aux données des sessions en ligne.

- Renseignements circonstanciels et contextuels collectés dans le cadre des activités d'un participant qui peuvent aider à évaluer s'il existe des motifs raisonnables de soupçonner qu'une opération est liée à une infraction applicable prévue à l'article 7 ou 7.1 de la Loi. Il peut s'agir, par exemple, de descriptions détaillées, d'analyses antérieures et d'évaluations effectuées par un participant, de mesures prises auparavant (comme le désengagement financier) ou de tout soupçon précédent de commission réelle ou tentée d'une infraction de blanchiment d'argent, de financement des activités terroristes ou de contournement des sanctions.

- Renseignements publics légalement collectés dans le cadre des activités d'un participant. Il peut s'agir, par exemple, de registres publics, de rapports des médias, de profils de médias sociaux, de divulgations financières, ou de publications spécialisées.

Pour garantir que les renseignements sont communiqués, collectés ou utilisés pour des fins qu'une personne raisonnable considérerait comme appropriées dans les circonstances, le participant au Code veillera à ce que la communication, la collecte et l'utilisation soient nécessaires pour atteindre les fins détaillées dans la section 3. Tout préjudice susceptible d'en résulter est proportionnel aux avantages obtenus; et les fins ne peuvent pas être atteintes efficacement par la transmission de moins de renseignements personnels.

4. Manière de transmettre des renseignements personnels

Les renseignements personnels pertinents seront communiqués, collectés ou utilisés à l'aide de l'une des méthodes sécurisées mentionnées ci-dessous qui assurent une confidentialité conforme à la LPRPDE et à la section 5 du Code.

- Méthodes de communication **électronique ou virtuelle sécurisée**, comme les courriels chiffrés, l'utilisation d'API, de salles de données virtuelles et de réseaux de collaboration sécurisés, les services de transfert de fichiers sécurisés, ou les protocoles de technologie de l'information.

- Méthodes de communication **physique ou de personne à personne sécurisée**, comme les lignes téléphoniques sécurisées, les vidéoconférences sécurisées, ou le courrier recommandé.

Ces mesures garantiront la protection des renseignements personnels pertinents contre la perte, l'accès non autorisé lors de la communication ou l'accès non autorisé lors de l'utilisation. Si les renseignements personnels pertinents ne sont pas considérés comme étant exacts, le ou les participants peuvent prendre des mesures raisonnables pour informer un participant concerné et corriger ces renseignements dans la mesure du possible.

5. Mesures visant à protéger les renseignements personnels communiqués, collectés ou utilisés

Remarque : Les demandeurs doivent détailler autant que possible les mesures visant à garantir la protection des renseignements personnels, entre autres en faisant référence aux normes reconnues de leur secteur d'activité (comme celles du BSIF, du NIST ou d'ISO) auxquelles les participants adhèrent pour démontrer que les renseignements personnels sont protégés de manière adéquate.

Conservation et élimination

Afin de garantir la protection des renseignements personnels pertinents communiqués, collectés ou utilisés parmi les participants, les renseignements ne sont conservés que pour la durée nécessaire à leur utilisation, conformément aux fins décrites, ou aux politiques de conservation propres aux participants concernant l'information relative au blanchiment d'argent, au financement des activités terroristes ou au contournement des sanctions, comme celles exigées par la Loi et les règlements connexes.

Les participants mettront en place des mécanismes garantissant que les renseignements personnels ne sont pas conservés plus longtemps que cela est nécessaire. Les participants élimineront les renseignements personnels de manière à ce qu'ils ne soient plus accessibles ou utilisables. Les moyens d'élimination peuvent inclure, entre autres, l'effacement des données, les logiciels de suppression sécurisée ou la destruction physique.

Remarque : Les demandeurs doivent inclure un calendrier de conservation de tous les renseignements personnels collectés, utilisés et communiqués, conformément à l'article 11.01 de la Loi.

Tenue de documents

Les participants au présent Code tiendront des documents, conformément aux exigences du *Règlement sur le recyclage des produits de la criminalité et le financement des activités terroristes* et de la LPRPDE. Ces exigences comprennent la tenue de documents ou de copies de documents en format lisible par machine ou électronique si une copie papier peut facilement être produite à partir de celle-ci. Des copies physiques des documents peuvent également être conservées.

Les participants conserveront les renseignements dans des documents électroniques, des documents physiques ou des enregistrements de manière à ce qu'ils soient lisibles ou perceptibles par toute personne autorisée à avoir accès aux documents ou aux enregistrements.

Aux fins de tenue de documents, les participants consigneront, classeront et catégoriseront les renseignements personnels pertinents. Les participants consigneront et conserveront également l'information relative aux décisions de communiquer, de collecter ou d'utiliser des renseignements personnels, ainsi que les raisons justifiant ces décisions, en tenant compte des critères pertinents définis dans les cadres établis.

Les participants conserveront les documents et les renseignements personnels pertinents de manière à permettre l'identification de leur origine.

Mesures de protection

Les renseignements personnels pertinents devant être conservés et échangés seront protégés par des mesures adaptées à leur degré de confidentialité. Puisque les renseignements personnels en question seront souvent de nature très délicate, ceux communiqués, collectés et utilisés conformément au présent Code seront protégés par de solides mesures.

Les participants au présent Code de pratique suivront des procédures internes d'évaluation pour déterminer le niveau de confidentialité à attribuer aux renseignements personnels pertinents.

Les participants au Code effectueront des évaluations afin de cerner les vulnérabilités et les menaces associées aux renseignements pendant qu'ils sont conservés et communiqués. Les participants mettront en place des mesures de sécurité adaptées à la confidentialité des renseignements personnels à transmettre ou à utiliser pour répondre aux risques et aux menaces cernées.

Les formats physiques des renseignements personnels pertinents seront conservés dans des environnements physiques sécurisés qui peuvent inclure, entre autres, des classeurs verrouillés ou un coffre-fort. Les formats numériques des renseignements personnels pertinents seront conservés dans des espaces sécurisés et transmis au moyen de mécanismes sécurisés, avec des formes physiques et numériques de contrôle des accès. Ces contrôles peuvent inclure le chiffrage (pendant la transmission des renseignements et lorsque ces derniers sont non utilisés), des logiciels d'authentification multifactorielle, la gestion de clés, des autorisations de contrôle des accès basés sur les rôles et d'autres types d'algorithmes de chiffrement actuellement utilisés par les programmes de lutte contre le blanchiment d'argent et le financement des activités terroristes des participants.

L'accès aux formats numériques ou physiques des renseignements personnels pertinents sera limité en fonction de la nécessité et des autorisations associées aux rôles. Les mesures visant à protéger les renseignements personnels peuvent inclure, entre autres, la surveillance des registres des accès ou des pistes de vérification, des systèmes de détection des intrusions, des contrôles des accès basés sur les rôles et d'autres méthodes raisonnables.

Les protections supplémentaires en matière de conservation et d'échange doivent inclure des méthodes reconnues et sécuritaires de protection des renseignements, comme des protocoles d'authentification à deux facteurs; la génération, la distribution, la rotation et le stockage sécurisés des clés de chiffrement; et des protocoles informatiques sur des architectures de réseau sécurisées. Les mesures de protection doivent également inclure des procédures et protocoles reconnus de gestion du personnel, de gestion des risques et de gestion de la confidentialité visant à protéger les renseignements pertinents tout au long de leur communication, de leur collecte ou de leur utilisation, comme des politiques de mots de passe forts, des mises à jour régulières des logiciels et la formation des employés sur la confidentialité et l'utilisation appropriées des renseignements. Les mesures de protection doivent également inclure des méthodes reconnues pour vérifier l'exactitude et l'intégralité des données, comme les pratiques de validation des données, les cadres internes de gouvernance des données ou la formation des employés.

Les participants limiteront l'accès aux renseignements et leur échange au sein de l'organisation. Les personnes qui interviennent dans l'accès ou la réception de renseignements doivent :

- avoir un rôle lié aux fonctions de lutte contre le blanchiment d'argent, le financement des activités terroristes et le contournement des sanctions des participants pour les renseignements communiqués, collectés ou utilisés en lien avec le Code, ou à toute fonction associée à la vérification ou à l'examen, aux aspects juridiques ou à la sécurité de l'information, ou à toute autre fonction organisationnelle pertinente pour les renseignements communiqués, collectés ou utilisés en lien avec le Code;
- suivre une formation sur la confidentialité et la lutte contre le blanchiment d'argent, le financement des activités terroristes et le contournement des sanctions;
- avoir accès au Code de pratique, l'avoir lu et le comprendre;
- connaître et appliquer les mécanismes autorisés de communication, de collecte et d'utilisation sécurisées des renseignements pertinents;
- appliquer toutes les politiques et procédures pertinentes pour assurer la confidentialité.

Réponse aux violations

En cas de violation des mesures de sécurité concernant les renseignements collectés conformément à la section 3 du présent Code, les participants suivront les protocoles de gestion des incidents de leur organisation. Ces protocoles doivent être conformes à la LPRPDE et aux autres lois applicables et doivent prévoir, sans s'y limiter, le confinement immédiat, l'enquête et l'évaluation pour déterminer la raison et l'étendue de la violation, l'évaluation des risques pour déterminer le préjudice, l'identification des personnes touchées et la communication avec les autorités compétentes, ainsi que la mise en place de mesures visant à empêcher qu'une violation semblable ne se reproduise.

Si une violation se produit après que les renseignements personnels ont été collectés auprès d'un autre participant au Code, le participant au Code destinataire est responsable des

protocoles de gestion des incidents. Le participant au Code destinataire informera le participant lui ayant transmis les renseignements de toute violation liée à ce qui a été communiqué. Si la violation se produit pendant la communication ou si elle est de responsabilité conjointe dans le cadre d'un mécanisme d'échange de données, les participants veilleront à ce que les politiques et procédures appropriées soient appliquées, y compris les protocoles de gestion des incidents et les procédures d'avis.

Si l'on croit qu'une violation des mesures de protection des renseignements personnels entraîne un risque réel de préjudice important pour une personne, le ou les participants concernés suivront les procédures établies pour se conformer aux articles 10.1, 10.2 et 10.3 de la LPRPDE et aux lois provinciales pertinentes, notamment en signalant la violation au Commissariat à la protection de la vie privée du Canada ou aux autorités provinciales compétentes, ainsi qu'aux personnes touchées.

6. Respect des exigences de la Loi

Les fins définies dans le présent Code de pratique sont directement liées à l'article 3 de la Loi. L'objectif de l'échange de renseignements personnels pertinents est conforme à l'article 3 de la Loi qui souligne la nécessité de mettre en place des mesures précises pour détecter et décourager le blanchiment d'argent et le financement des activités terroristes et pour faciliter les enquêtes et les poursuites relatives aux infractions de blanchiment d'argent, de financement des activités terroristes et de contournement des sanctions.

Les renseignements personnels pertinents transmis peuvent aussi permettre de mieux répondre à la menace que représente le crime organisé en offrant l'information nécessaire pour le priver des produits de ses activités criminelles, tout en veillant à ce que des mesures de protection appropriées soient en place pour protéger la vie privée des personnes à l'égard de leurs renseignements personnels.

Le présent Code s'harmonise aussi avec les exigences de la Loi, dans la mesure où il soutient les engagements internationaux du Canada et renforce la capacité du pays à prendre des mesures ciblées pour protéger son système financier et atténuer le risque que le blanchiment d'argent et le financement des activités terroristes font peser sur lui.

Les éléments du présent Code de pratique sur la conservation et la tenue de documents respectent l'article 6 de la Loi et les règlements connexes. Les processus, mesures et protocoles décrits dans le présent Code soulignent que ce dernier répond, ou même dépasse, les attentes liées à la tenue de documents et à la conservation des renseignements pertinents pour la lutte contre le blanchiment d'argent, le financement des activités terroristes ou le contournement des sanctions associées à la Loi et aux règlements connexes.

Le présent Code de pratique respecte les limites de communication énoncées à l'article 8 de la Loi et s'harmonise avec les dispositions relatives à la communication, à la collecte, à l'utilisation et à l'immunité figurant à l'article 11.01 de la Loi. Pour les dispositions particulières, veuillez consulter l'annexe C du présent Code.

Le présent Code de pratique permettra aux participants de s'assurer qu'ils satisfont aux exigences de l'article 7 ou 7.1 de la Loi.

Aucun participant ne doit révéler qu'il a communiqué, collecté ou utilisé tout renseignement personnel pertinent aux fins décrites dans le présent Code de pratique dans l'intention de nuire illégalement à une enquête criminelle, qu'elle ait été ouverte ou non.

7. Dispositions visant à assurer une protection des renseignements personnels sensiblement identique ou supérieure à celle prévue par la LPRPDE

Principe 1 : Responsabilité

Seules les personnes autorisées auprès de chaque participant peuvent intervenir dans la communication, la collecte et l'utilisation des renseignements. Tous les participants s'engagent à mettre en place des programmes complets de protection de la confidentialité et de lutte contre le blanchiment d'argent et le financement des activités terroristes afin de garantir le respect de toutes les lois applicables.

Tous les participants ont accepté les modalités du présent Code de pratique.

Le demandeur a mis ou mettra en place des mesures conformes aux exigences de responsabilité de la LPRPDE afin de garantir le respect des exigences en matière de confidentialité énoncées dans le présent Code. Ces mesures comprennent, entre autres, des méthodes sécurisées d'échange de renseignements personnels, des mesures de conservation et d'élimination, la tenue de documents, des politiques d'intervention en cas de violation et des mesures de protection, comme l'accès limité à certains rôles.

Chaque participant rendra également disponible le nom ou le titre, ainsi que l'adresse, de la personne responsable des politiques et pratiques de l'organisation en matière de confidentialité et à laquelle les plaintes ou les demandes de renseignements peuvent être adressées.

Principe 2 : Détermination des fins

La section 2 du présent Code de pratique détermine les fins de l'échange de renseignements pertinents, qui sont conformes aux exigences législatives et réglementaires du Canada en matière de lutte contre le blanchiment d'argent et le financement des activités terroristes.

Principe 3 : Consentement

Le présent Code porte sur la collecte, l'utilisation ou la communication lorsque les parties ont décidé que le consentement n'est pas nécessaire conformément au paragraphe 11.01(1) de la Loi.

Principe 4 : Limitation de la collecte

Remarque : Les demandeurs doivent indiquer précisément les politiques et procédures qui ont été ou qui seront mises en place afin d'éviter toute collecte excessive, et décrire précisément la manière dont les parties veilleront à ce que les renseignements communiqués, et donc ceux collectés par le destinataire, n'aillent pas au-delà de ce qui est nécessaire aux fins établies.

Les participants ne collecteront des renseignements personnels dans le cadre du présent Code de pratique que pour respecter leurs obligations actuelles en matière de lutte contre le blanchiment d'argent et le financement des activités terroristes et uniquement aux fins prévues par le présent Code.

Principe 5 : Limitation de l'utilisation, de la communication et de la conservation

Seules certaines personnes auprès de chaque participant peuvent utiliser, communiquer et collecter des renseignements personnels dans le cadre du présent Code de pratique, dans le respect des limites et des contrôles énoncés à la section 5 ci-dessus. Les participants ne doivent pas utiliser, communiquer ou conserver des renseignements personnels dans le cadre du présent Code, sauf à des fins particulières décrites à la section 3 du présent Code. Les participants doivent mettre en place des procédures pour contourner l'élimination prévue des renseignements personnels lorsqu'il peut être légalement nécessaire de les conserver.

Principe 6 : Exactitude

Remarque : Le demandeur doit préciser la manière dont il s'assurera que les renseignements sont exacts et complets, en particulier dans un contexte où les renseignements doivent être ou ont été transmis à un ou à plusieurs participants. Cela peut inclure, entre autres, l'évaluation de la fiabilité des sources à partir desquelles les renseignements personnels peuvent être collectés, et les processus en place pour mettre à jour les renseignements qui peuvent être, ou ont pu être, échangés.

Le présent Code de pratique indique que les participants doivent disposer de méthodes permettant de s'assurer que les renseignements sont suffisamment exacts, à jour et complets pour les fins auxquelles ils sont utilisés, en tenant compte des intérêts de la personne concernée. Si un participant détermine que les renseignements en question ne sont pas suffisamment exacts, complets ou à jour, le présent Code exige que les participants prennent des mesures raisonnables pour aviser les autres participants que les renseignements sont inexacts et les corriger le cas échéant.

Principe 7 : Mesures de sécurité

La section 5 du présent Code de pratique décrit les mesures de protection qui doivent être appliquées par les participants au Code. La section 5 décrit également les mesures relatives à la tenue de documents, à la réponse en cas de violation, à la conservation et à l'élimination.

Principe 8 : Transparence

Tous les participants au présent Code de pratique disposent d'une documentation facilement accessible, publique et compréhensible qui explique les politiques de confidentialité de chaque participant en matière de renseignements personnels.

Principe 9 : Accès aux renseignements personnels

Les participants au présent Code de pratique doivent appliquer des politiques et procédures afin d'assurer un accès conforme aux exigences prévues par la LPRPDE et des lois provinciales

pertinentes en matière de protection de la vie privée. Ces procédures prévoient la réalisation d'une recherche raisonnable pour relever les documents pertinents, l'examen de l'applicabilité des exemptions possibles et la fourniture d'une réponse à la demande, y compris tout document pertinent, dans les délais prévus par la législation applicable. Le processus tiendra également compte du fait que l'objectif du Code est de garantir la communication des renseignements personnels à l'insu ou sans le consentement de la personne concernée.

Les participants mettront en place un protocole et un processus afin de déterminer la coordination et les responsabilités appropriées lorsqu'une demande concerne l'accès à des renseignements qui ont été transmis par un participant à un ou plusieurs autres participants.

Principe 10 : Possibilité de porter plainte à l'égard du non-respect des principes

> **Remarque :** Le demandeur doit expliquer les procédures permettant à une personne de déposer une plainte auprès d'un participant, ainsi que celles de traitement des plaintes, en particulier lorsque la plainte concerne des renseignements communiqués à un autre participant, ou provenant de celui-ci, ou lorsque les renseignements sont détenus conjointement.

Toute personne ou entité qui estime qu'un participant n'a pas respecté l'un des éléments du présent Code de pratique peut déposer une plainte auprès du Commissariat à la protection de la vie privée ou du participant concerné. Les participants au Code mettront en place un protocole et un processus pour accepter, examiner et traiter les plaintes et demandes de renseignements relatives à la protection de la vie privée qui sont conformes à la LPRPDE et aux autres lois pertinentes en matière de protection de la vie privée, et pour répondre à ces plaintes et demandes.

Annexe A : Participants au Code

Participant 1 : Dénomination sociale et commerciale

Numéro de l'entité déclarante :

Coordonnées :

John Smith

Dirigeant principal de la conformité

jsmith@participant1.ca

555-555-5555

123 Road Road, Toronto (Ontario), M5M 1R5, CANADA

Participant 2 : Dénomination sociale et commerciale

Numéro de l'entité déclarante :

Coordonnées :

Jane James

Dirigeante principale de la conformité

jjames@participant2.ca

555-555-5555

456 Road Road, Ottawa (Ontario), K1H 1H1, CANADA

Annexe B : Définition de « renseignement personnel »

LPRPDE, paragraphe 2(1) :

« ***renseignement personnel*** Tout renseignement concernant un individu identifiable. »

Annexe C : Article 11.01 de la Loi

Communication sans le consentement de l'intéressé

11.01 (1) La personne ou l'entité visée à l'article 5 peut, si les conditions ci-après sont réunies, communiquer à une autre personne ou entité visée à cet article les renseignements personnels d'un individu, à son insu ou sans son consentement :

a) les renseignements ont été recueillis dans le cadre de ses activités;

b) il est raisonnable de communiquer ces renseignements en vue de détecter ou de décourager le recyclage des produits de la criminalité, le financement des activités terroristes ou le contournement des sanctions;

c) la communication de ces renseignements effectuée au su ou avec le consentement de l'individu risquerait de compromettre la capacité de détecter ou de décourager le recyclage des produits de la criminalité, le financement des activités terroristes ou le contournement des sanctions;

d) la communication est faite conformément aux règlements.

Collecte et utilisation

(2) La personne ou l'entité visée à l'article 5 peut recueillir ou utiliser les renseignements qui lui sont communiqués au titre du paragraphe (1) à l'insu de l'individu ou sans son consentement, si la collecte ou l'utilisation est faite en conformité avec les règlements.

Immunité

(3) Nul ne peut être poursuivi pour avoir, de bonne foi, communiqué un renseignement au titre du paragraphe (1) ou recueilli ou utilisé un renseignement au titre du paragraphe (2).