Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Avis de mise en œuvre sur la protection des renseignements personnels 2023-03 : Orientation relative à la collecte, à l'utilisation, à la conservation et à la divulgation de renseignements personnels accessibles au public en ligne

Publié : le 2023-07-24

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT39-77/2023F-PDF
ISBN: 978-0-660-67780-4

Ce document est disponible sur le site Web du gouvernement du Canada à l'adresse www.canada.ca

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Privacy Implementation Notice 2023-03: Guidance pertaining to the collection, use, retention and disclosure of personal information that is publicly available online

Avis de mise en œuvre sur la protection des renseignements personnels 2023-03 : Orientation relative à la collecte, à l'utilisation, à la conservation et à la divulgation de renseignements personnels accessibles au public en ligne

1. Date d'entrée en vigueur

Le présent Avis de mise en œuvre entre en vigueur le 1er août 2023.

2. Pouvoirs

Le présent Avis de mise en œuvre est émis en vertu de l'alinéa 71(1)*(d)* de la *Loi sur la protection des renseignements personnels*.

3. Objectif

Le présent Avis de mise en œuvre fournit une orientation conformément aux exigences de la *Loi sur la protection des renseignements personnels* et des instruments de politique connexes aux responsables en matière de

protection des renseignements personnels des institutions gouvernementales en ce qui concerne la collecte, l'utilisation, la communication et la conservation des renseignements personnels accessibles au public en ligne. Le présent Avis est également destiné à servir de ressource partageable avec les secteurs de programmes, qui peuvent l'utiliser pour guider leurs activités et élaborer leurs propres politiques et procédures internes. La présente orientation vise à compléter les politiques institutionnelles existantes. Bien qu'elle ne traite pas des renseignements accessibles au public provenant d'autres sources, comme la presse écrite ou la télévision, une grande partie des renseignements qu'elle contient s'appliquent à d'autres médias.

4. Contexte

Les institutions gouvernementales recueillent, utilisent, conservent et divulguent, c'est-à-dire gèrent, des renseignements personnels accessibles au public en ligne à diverses fins, comme :

- la sensibilisation et la communication publique [1];
- la recherche, l'examen des tendances et l'établissement des questions émergentes;
- les activités à l'appui de la sécurité nationale, de l'application de la loi et des enquêtes administratives.

5. Orientation

5.1 Exigences existantes

S'il existe une forte probabilité qu'une personne, seule ou au moyen d'autres renseignements, puisse être identifiée, il est possible que ces renseignements contiennent des renseignements personnels au sens de

l'article 3 de la *Loi sur la protection des renseignements personnels*.

Les renseignements personnels accessibles au public en ligne devraient, dans la plupart des cas, être traités de la même façon que tout autre renseignement personnel détenu par les institutions gouvernementales. Les considérations suivantes concernent spécifiquement les renseignements personnels disponibles en ligne.

5.1.1 Collecte de renseignements personnels accessibles au public en ligne

Pouvoir de recueillir

Comme le décrit l'article 4 de la *Loi sur la protection des renseignements personnels*, les renseignements personnels ne peuvent être recueillis que s'ils sont directement liés à un programme ou à une activité de l'institution. Cette exigence s'applique indépendamment du fait que les renseignements personnels soient accessibles au public ou non; les institutions doivent toujours veiller à ce qu'elles aient l'autorisation légale de recueillir les renseignements avant de le faire. L'autorisation légale d'un programme ou d'une activité est généralement contenue dans une loi du Parlement ou dans des règlements ultérieurs. L'approbation des dépenses proposées dans le budget des dépenses et l'autorisation par une loi de crédits peuvent être une indication de l'autorisation légale d'un programme ou d'une activité.

Collecte directe

Lorsque des renseignements personnels sont nécessaires à des fins administratives, la collecte directe est la règle par défaut, sauf dans des circonstances particulières. Comme indiqué au paragraphe 5(3) de la *Loi sur la protection des renseignements personnels*, la collecte directe n'est pas nécessaire si les renseignements personnels ne sont pas utilisés à des fins

administratives. Cela pourrait entraîner la collecte de renseignements inexacts; ou cela irait à l'encontre de l'objectif ou porterait préjudice à l'utilisation pour laquelle les renseignements sont recueillis. De plus, il convient de tenir compte de l'exception prévue au paragraphe 5(1) de la *Loi*, qui stipule que la collecte ne doit pas être directe lorsque la personne l'autorise autrement ou lorsque les renseignements personnels peuvent être communiqués à une institution en vertu du paragraphe 8(2). Avant que les renseignements personnels obtenus en ligne ne soient utilisés à des fins administratives, les personnes concernées par ces renseignements doivent avoir la possibilité de les examiner et de les corriger si nécessaire. Cela peut ne pas être approprié dans tous les cas, par exemple lorsque la personne concernée fait l'objet d'une enquête active. Dans les cas où l'institution ne consulterait pas la personne concernée, elle serait toujours liée par l'obligation d'exactitude stipulée à l'article 6(2) de la *Loi*. Pour les décisions administratives, il n'est pas recommandé de s'appuyer uniquement sur des renseignements personnels recueillis à partir de sources en ligne accessibles au public.

Limiter la collecte

Même lorsque les renseignements personnels sont accessibles au public en ligne, les institutions doivent limiter la collecte de ces renseignements à ce qui est directement lié et nécessaire aux programmes ou aux activités de l'institution gouvernementale, comme le prévoit le point 4.2.9 de la *Directive sur les pratiques relatives à la protection de la vie privée*.

Lors d'une collecte manuelle de renseignements personnels à partir d'une source en ligne, les employés doivent évaluer chaque élément de renseignement personnel ayant été recueilli afin de déterminer s'il correspond à ces critères. Cela peut s'avérer impossible dans certains cas

où des éléments de renseignements personnels sont imbriqués dans d'autres. Néanmoins, les institutions devraient limiter leur collecte à ces éléments précis.

Lorsqu'elles utilisent des méthodes automatisées de collecte [2], les institutions doivent consulter les responsables en matière de protection des renseignements personnels de leur ministère pour savoir comment ajuster les paramètres de collecte du logiciel pour limiter la collecte aux seuls éléments nécessaires au programme ou à l'activité. Cela réduit la probabilité d'une collecte excessive. En cas de collecte excessive, les institutions doivent faire appel à leurs responsables en matière de protection des renseignements personnels pour évaluer les incidences potentielles sur l'institution ou les personnes concernées, et procéder à la mise en œuvre des mesures d'atténuation qui s'imposent, et qui peuvent inclure l'élimination des renseignements superflus.

En règle générale, les renseignements personnels divulgués en ligne par inadvertance, fuite, piratage ou vol ne doivent pas être considérés comme étant accessibles au public, car la divulgation, par sa nature même, aurait eu lieu à l'insu ou sans le consentement de la personne à laquelle les renseignements personnels se rapportent, empiétant ainsi sur une attente raisonnable de protection des renseignements personnels. Les institutions doivent faire appel à leurs services juridiques si elles soupçonnent que les renseignements personnels qu'elles envisagent de recueillir correspondent à ce scénario.

Présence d'un fichier de données personnelles

Les institutions doivent établir les éléments de renseignements personnels qu'elles recueillent à partir de sources en ligne accessibles au public dans un fichier de données personnelles (FDP) si ces renseignements sont destinés à un usage administratif ou si ces renseignements sont organisés

de façon à pouvoir être repérés à partir du nom d'une personne, d'un numéro ou d'un symbole d'identification qui lui a été attribué. Lorsque des renseignements personnels sont utilisés dans le cadre d'activités de communication, les institutions peuvent s'appuyer sur les FDP standards suivants : POU 938 (Activités de sensibilisation) et POU 914 (Communications publiques). Si des renseignements personnels accessibles au public sont recueillis pour un nouvel usage, ou si un programme ou une activité nécessite la collecte de nouveaux éléments de renseignements personnels, il peut être nécessaire d'enregistrer ou de procéder à la mise à jour d'un FDP précis à l'institution qui reflète mieux les éléments de renseignements recueillis, l'objectif de la collecte et la période de conservation.

Avis de collecte

Les personnes doivent être informées si leurs renseignements personnels sont recueillis à l'appui d'une décision administrative qui les concerne directement, sauf si la notification risque d'entraîner la collecte de renseignements inexacts ou d'aller à l'encontre de l'objectif ou de l'utilisation pour laquelle les renseignements sont recueillis. Cette exigence continue de s'appliquer aux renseignements personnels accessibles au public en ligne. Les institutions doivent consulter la section 4.2.10 de la *Directive sur les pratiques relatives à la protection de la vie privée*pour connaître les éléments qui doivent figurer dans une déclaration de confidentialité.

Lorsque des renseignements personnels accessibles au public en ligne sont recueillis indirectement à des fins non administratives, les institutions peuvent informer indirectement les personnes de la collecte au moyen d'avis publiés par l'entremise des sites Web ou des comptes de médias sociaux des institutions. L'avis permet aux utilisateurs en ligne de

comprendre comment l'institution recueille et utilise les renseignements personnels qui sont accessibles au public en ligne dans le cadre de son mandat, et donne aux personnes la possibilité de demander d'avoir accès aux renseignements recueillis. Les institutions devraient avoir recours à des mesures de transparence supplémentaires lorsqu'il est possible de le faire, afin d'assurer une portée plus vaste.

Utilisation de fournisseurs de services ou de données tiers

Les organisations du secteur privé sont soumises à leurs propres obligations en ce qui concerne la collecte, l'utilisation et la divulgation des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, et des lois provinciales sur la protection de la vie privée. Les institutions du gouvernement fédéral, quant à elles, assument la responsabilité ultime, en vertu de la *Loi sur la protection des renseignements personnels*, lorsqu'elles font appel à des fournisseurs de services ou de données tiers pour la gestion des renseignements personnels accessibles au public en ligne. Ces responsabilités, décrites dans le présent Avis, continuent de s'appliquer lorsqu'il s'agit d'obtenir des renseignements personnels auprès de tiers par l'entremise d'une demande, d'un abonnement ou d'un achat. Les contrats, les ententes ou les arrangements conclus avec des fournisseurs de services ou de données tiers doivent décrire clairement les mesures prises pour protéger les renseignements personnels, conformément aux exigences de la *Loi sur la protection des renseignements personnels* et des instruments politiques connexes, y compris l'obligation d'informer immédiatement l'institution gouvernementale d'une atteinte à la vie privée, le cas échéant.

Lorsqu'elles font appel à un service ou à un fournisseur de données tiers, les institutions doivent veiller à ce qu'ils aient obtenu, de façon légitime et légale, les renseignements personnels qui seront fournis à l'institution. De plus, bien que ce ne soit pas une obligation, on encourage les institutions à tenir compte des antécédents du tiers en matière d'incidents liés à la protection des renseignements personnels. Pour obtenir de plus amples renseignements sur la mobilisation de tiers, veuillez consulter le Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché.

5.1.2 Utilisation et divulgation

Conformément à l'article 69(2) de la *Loi sur la protection des renseignements personnels*, les renseignements personnels accessibles au public ne sont pas soumis aux restrictions d'utilisation et de divulgation prévues aux articles 7 et 8 de cette *Loi*. Toutefois, dès que les renseignements personnels cessent d'être accessibles au public, ils sont soumis aux exigences d'utilisation et de divulgation des articles 7 et 8. Cela signifie que les institutions ne peuvent plus, sans le consentement de la personne concernée, utiliser les renseignements personnels autrement que pour l'objectif pour lequel ils ont été obtenus à l'origine ou pour une utilisation compatible avec cet objectif. Les responsables de programmes devront évaluer dans quelle mesure les renseignements sont accessibles au public au moment où il est prévu de les divulguer. Il s'agit notamment de vérifier, dans la mesure du possible, si les renseignements à divulguer sont **identiques** à ceux qui sont dans le domaine public au moment précis de la divulgation. De plus, les déclarations de confidentialité doivent être mises à jour pour inclure les utilisations supplémentaires des renseignements recueillis, en particulier si les nouvelles utilisations diffèrent de façon significative de ce qui était décrit dans la déclaration initiale. Enfin, les

institutions doivent respecter les exigences énoncées dans la *Directive sur les pratiques relatives à la protection de la vie privée* en ce qui concerne l'exactitude des renseignements et la mise en place de garanties pour leur utilisation, leur divulgation et leur conservation.

Vérification de l'exactitude

Comme l'exige la *Loi sur la protection des renseignements personnels*, les institutions doivent veiller à ce que les renseignements personnels recueillis à des fins administratives soient aussi exacts, à jour et complets que possible. Cette exigence s'applique aux renseignements personnels qui sont accessibles au public en ligne lorsqu'ils sont utilisés dans le cadre d'un processus décisionnel. Pour commencer, la collecte de renseignements personnels directement auprès de la personne concernée diminue la probabilité d'inexactitudes.

La *Directive sur les pratiques relatives à la protection de la vie privée* vient augmenter l'obligation d'exactitude de la *Loi,* en exigeant également que les institutions documentent la source ou la technique utilisée pour valider l'exactitude des renseignements personnels, et qu'elles les identifient dans la description du fichier de données personnelles connexe. Cela peut s'avérer particulièrement difficile dans le domaine du numérique, compte tenu de l'augmentation de la désinformation. Afin d'atténuer les risques connexes, les institutions devraient consulter plusieurs sources lorsqu'elles recueillent des renseignements personnels en ligne, en particulier lorsque ces renseignements ne proviennent pas de la personne concernée comme telle. Les institutions devraient mettre en place un processus permettant de déterminer les niveaux de confiance liés à l'exactitude, à l'imputabilité et à la véracité des renseignements. Cela peut comprendre le fait de vérifier les renseignements auprès d'autres sources ou directement auprès de la personne concernée. Quel que soit le degré de confiance, les

renseignements personnels obtenus à partir d'une source en ligne accessible au public ne doivent généralement pas être utilisés seuls à des fins administratives. Lorsque des renseignements personnels sont recueillis à des fins non administratives, comme l'observation des tendances et des récits en ligne, les institutions doivent veiller à ce que les renseignements soient aussi précis que nécessaire pour cet objectif en particulier.

Garanties

La disponibilité publique des renseignements personnels en ligne n'exempte pas les institutions des obligations liées à la protection de ces renseignements. Ceci est particulièrement important dans les situations où des renseignements personnels accessibles au public sont combinés pour créer un profil potentiellement élargi. Même lorsque les renseignements personnels sont accessibles au public en ligne et qu'ils peuvent être utilisés à d'autres fins que celles pour lesquelles ils ont été recueillis à l'origine, les institutions doivent en limiter l'accès aux personnes qui en ont besoin pour exercer des fonctions ou des tâches liées à un programme ou à une activité. Des garanties administratives, techniques et physiques doivent continuer à être utilisées pour protéger les renseignements. De plus, comme l'exige la *Politique sur la protection de la vie privée* (consulter4.2.1), les employés doivent être informés des politiques, des procédures et des exigences légales en vertu de la *Loi sur la protection des renseignements personnels* avant d'être autorisés à accéder à tout renseignement personnel ayant été recueilli, même si ce renseignement personnel est largement disponible en ligne. En outre, comme pour tout autre renseignement personnel, les institutions doivent mettre en place des mesures appropriées pour garantir que l'accès aux renseignements personnels est contrôlé et documenté à des fins de responsabilisation.

5.1.3 Conservation

Conformément au paragraphe 4(1)(a) du *Règlement sur la protection des renseignements personnels*, tous les renseignements personnels utilisés à des fins administratives, qu'ils aient été obtenus à partir de sources en ligne accessibles au public ou non, doivent être conservés pendant au moins deux ans. Cette période de conservation permet aux personnes d'exercer leur droit d'accès en vertu de la *Loi sur la protection des renseignements personnels*. Sous réserve d'autres obligations juridiques ou politiques, les renseignements personnels utilisés à des fins non administratives doivent être éliminés dès qu'ils ne sont plus nécessaires au programme ou à l'activité. Les institutions doivent examiner régulièrement les renseignements et déterminer s'il est nécessaire de les conserver. Dans tous les cas, des périodes de conservation claires, associées à des mesures de contrôle d'accès et à des pistes d'audit solides, peuvent contribuer à atténuer les risques en matière de protection des renseignements personnels. De plus, lorsqu'elles conservent des renseignements personnels obtenus à partir d'une source en ligne accessible au public, les institutions devraient envisager d'étiqueter les renseignements comme étant « accessibles au public en ligne », et d'indiquer la date et la source de la collecte. Ce faisant, elles pourront ainsi veiller à ce que toute utilisation future des renseignements tienne compte de leur source, et les traite en conséquence.

5.2 Obligations juridiques supplémentaires

Il existe un risque que la collecte de renseignements personnels accessibles au public en ligne entraîne des obligations juridiques allant au-delà de celles prévues par la *Loi sur la protection des renseignements personnels*. Par exemple, certaines institutions sont soumises à des règles spéciales énoncées dans la législation et les politiques ministérielles qui leur sont propres, et toutes les institutions doivent se conformer à la *Charte*

canadienne des droits et libertés. Les institutions devraient consulter leurs services juridiques pour déterminer dans quelle mesure leurs pratiques en matière de renseignements personnels peuvent comporter des exigences juridiques et applicables, et élaborer des mesures de conformité en conséquence.

De plus, il est important de prendre note que, bien que les conditions générales et/ou les contrats de licence d'utilisateur final des plateformes de médias sociaux ou d'autres sources en ligne diffèrent les uns des autres, certains interdisent à une institution de recueillir des renseignements personnels accessibles au public à certaines fins. Une personne qui consulte ou recueille du contenu sur ces plateformes, y compris des renseignements personnels, peut être considérée comme ayant accepté les conditions d'utilisation de la plateforme en question, même si une inscription ou une ouverture de séance est contournée ou n'est pas nécessaire pour accéder au contenu.

Certaines des conditions d'utilisation de certaines plateformes interdisent explicitement l'utilisation de leur contenu par toute personne associée à une entité gouvernementale ou agissant en son nom, et peuvent même interdire spécifiquement les actions liées à la surveillance ou à la collecte de tout renseignement. Il faut donc tenir compte des conditions d'utilisation avant de procéder à la collecte. Les institutions devraient collaborer avec leurs services juridiques afin d'entreprendre un examen détaillé de toute activité de collecte proposée, en combinaison avec les conditions d'utilisation précises associées à chaque plateforme à laquelle elles souhaitent faire appel. On encourage les institutions à procéder à la mise à jour de cette évaluation au fur et à mesure que les conditions d'utilisation changent. Les services juridiques des institutions peuvent également les aider à cerner d'autres risques juridiques, notamment les violations

potentielles des droits d'auteur causées par la copie non autorisée du contenu de la plateforme ou d'autres risques liés au contournement des mesures de protection technologiques.

5.3 Mesures de protection des renseignements personnels

Cette section aborde les pratiques qui peuvent contribuer à la protection des renseignements personnels lors de la gestion de ces derniers lorsqu'ils sont accessibles au public en ligne.

Autorisation de recueillir

L'élaboration d'une procédure d'autorisation de recueillir des renseignements, et la clarification des utilisations ultérieures autorisées, peuvent constituer une mesure de protection utile pour gérer les risques en matière de protection des renseignements personnels. La collecte de renseignements personnels à partir de sources en ligne comprend différents degrés d'atteinte à la vie privée. Cela dépend de l'étendue et des méthodes de collecte, des caractéristiques de confidentialité de la plateforme précise où la recherche et la collecte ont lieu, ainsi que des attentes raisonnables des utilisateurs en matière de respect des renseignements personnels dans cet espace numérique en particulier. On encourage les institutions à élaborer une procédure claire en matière d'autorisation afin de recueillir des renseignements personnels qui sont accessibles au public en ligne, et qui précise le niveau d'autorisation requis (par exemple, gestionnaire/superviseur, directeur, directeur général), en fonction du degré d'atteinte à la vie privée de la collecte.

Évaluer les conséquences liées à la protection des renseignements personnels

Une évaluation des facteurs relatifs à la vie privée (ÉFVP) est requise conformément à la *Directive sur l'évaluation des facteurs relatifs à la vie privée* lorsque la collecte de renseignements personnels est effectuée à des fins administratives, y compris tout renseignement personnel accessible au public en ligne. Dans un contexte non administratif, comme la collecte de données à partir de médias sociaux, dans le seul but d'observer des tendances ou des récits en ligne, un protocole régissant l'utilisation des renseignements personnels doit être établi conformément au point 4.2.5 de la *Politique sur la protection de la vie privée*. Une ÉFVP peut également être justifiée pour les programmes ou les activités qui recueillent des renseignements personnels à partir de sources en ligne accessibles au public à des fins non administratives, mais dont l'étendue ou la nature de la collecte peut susciter des préoccupations en matière de protection des renseignements personnels. Les responsables de programmes doivent collaborer avec les responsables en matière de protection des renseignements personnels de leur institution, souvent situés au sein du bureau de l'accès à l'information et protection des renseignements personnels (AIPRP), afin de déterminer l'outil à utiliser pour cerner correctement les risques en matière de protection des renseignements personnels, ainsi que les mesures d'atténuation correspondantes.

Techniques de préservation de la vie privée

Lorsqu'elles traitent des renseignements personnels accessibles au public et obtenus en ligne, les institutions devraient envisager d'utiliser des techniques de préservation de la vie privée, comme la dépersonnalisation et la minimisation des données. Ces mesures peuvent contribuer à la protection des renseignements personnels dans le cadre des activités de communication et de sensibilisation, ainsi que de recherche et d'analyse. Pour obtenir de plus amples renseignements, les institutions peuvent

consulter l'Avis de mise en œuvre de la protection des renseignements personnels 2023-01 : Dépersonnalisation et l'Avis de mise en œuvre de la protection des renseignements personnels 2020-03 : protection des renseignements personnels lors de la diffusion de renseignements à propos d'un petit nombre de personnes.

Politiques internes

Les politiques internes au niveau de programmes, élaborées en consultation avec les responsables en matière de protection des renseignements personnels de l'institution, constituent une autre mesure importante qui peut contribuer à la réduction des risques en matière de renseignements personnels lors de la collecte de ces derniers à partir de sources en ligne accessibles au public. Une politique interne pourrait inclure les éléments essentiels suivants :

- une liste des activités pour lesquelles l'utilisation de renseignements personnels obtenus à partir de sources en ligne accessibles au public est autorisée ou non;
- un processus d'autorisation pour la collecte;
- toute limitation de la collecte afin de minimiser les risques en matière de renseignements personnels, en considérant idéalement non seulement ce qui est légalement autorisé, mais aussi ce qui est de nature à favoriser la confiance du public;
- les outils et les méthodes utilisés pour recueillir les renseignements;
- les procédures utilisées pour noter la source et la date de la collecte;
- les mesures opérationnelles nécessaires pour assurer le respect des lois et des politiques applicables, notamment en ce qui concerne l'exactitude et la collecte excessive.

Utilisation de comptes attribuables ou non attribuables

Lorsqu'ils obtiennent des renseignements personnels à partir de sources en ligne accessibles au public, les employés doivent utiliser des comptes attribuables à leurs institutions. Veuillez consulter l'Avis de mise en œuvre de la protection des renseignements personnels 2021-01 : Exigences en matière de protection de la vie privée dans les comptes de médias sociaux officiels pour obtenir de plus amples renseignements.

Les comptes non attribuables ne doivent être utilisés que par les institutions ayant un mandat précis d'enquête ou de collecte de renseignements, comme le stipule leur loi habilitante. On recommande aux institutions de consulter leurs services juridiques avant d'utiliser des comptes non attribuables, car les régimes de réglementation auxquels elles sont soumises pourraient avoir des exigences en matière de transparence. En cas d'utilisation de comptes non attribuables, les institutions devraient adopter les pratiques exemplaires suivantes :

- éviter d'utiliser des renseignements d'identification, par exemple la photo d'une personne choisie au hasard et trouvée en ligne, comme image de profil du compte [3]. Les institutions devraient plutôt s'appuyer sur des renseignements de synthèse;
- restreindre l'accès à ces comptes à certains employés en particulier qui ont un besoin professionnel évident de les utiliser. Veiller à ce que la création de ces comptes soit documentée et approuvée aux niveaux appropriés et en consultation avec les responsables en matière de protection des renseignements personnels et les services juridiques de l'institution;
- examiner la nécessité de tenir à jour ces comptes régulièrement et au cas par cas;
- veiller à ce que les comptes non attribuables soient associés à un employé en particulier et supprimés au départ de l'employé s'ils ne sont plus nécessaires.

6. Application

Le présent Avis de mise en œuvre s'applique aux institutions gouvernementales stipulées à l'article 3 de la *Loi sur la protection des renseignements personnels*, y compris les sociétés d'État mères et aux filiales en propriété exclusive de ces sociétés. Toutefois, le présent Avis ne s'applique pas à la Banque du Canada.

7. Références

Législation

- *Loi sur l'accès à l'information*
- *Loi sur le Service canadien du renseignement de sécurité*
- *Charte canadienne des droits et libertés*
- *Loi sur le Centre de la sécurité des télécommunications*
- *Code criminel*
- *Loi sur la protection des renseignements personnels et les documents électroniques*
- *Loi sur la protection des renseignements personnels*

Instruments politiques et orientations connexes du Conseil du Trésor

- *Directive sur l'évaluation des facteurs relatifs à la vie privée*
- *Directive sur les pratiques relatives à la protection de la vie privée*
- *Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels*
- *Ligne directrice sur les services et le numérique*
- *Politique sur la protection de la vie privée*
- *Politique sur les services et le numérique*

- Avis de mise en œuvre de la protection des renseignements personnels 2020-03 : Protection des renseignements personnels lors de la diffusion de renseignements à propos d'un petit nombre de personnes
- Avis de mise en œuvre de la protection des renseignements personnels 2021-01 : Exigences en matière de protection de la vie privée dans les comptes de médias sociaux officiels
- Avis de mise en œuvre de la protection des renseignements personnels 2023-01 : Dépersonnalisation
- Prise en compte de la protection des renseignements personnels avant de conclure un marché

8. Demandes de renseignements

Les membres du public peuvent communiquer avec le Secrétariat du Conseil du Trésor du Canada - Demandes de renseignements du public pour obtenir des renseignements sur le présent Avis de mise en œuvre.

Les employés des institutions gouvernementales peuvent communiquer avec leur coordonnateur (coordonnatrice) de l'accès à l'information et de la protection des renseignements personnels (AIPRP) pour obtenir des renseignements sur le présent Avis de mise en œuvre.

Les coordonnateurs (coordonnatrices) de l'AIPRP peuvent communiquer avec la Division de la protection de la vie privée et des données du Secrétariat du Conseil du Trésor du Canada pour obtenir des renseignements sur le présent Avis de mise en œuvre.

Annexe A : Définitions

objectif administratif

L’utilisation de renseignements personnels concernant une personne dans le cadre d’un processus de prise de décisions qui touche directement cette personne (consulter l’article 3, *Loi sur la protection des renseignements personnels*). Cela comprend, sans toutefois s’y limiter, toutes les utilisations de renseignements personnels visant à confirmer l’identité (c’est-à-dire à des fins d’authentification et de vérification) et à déterminer l’admissibilité des personnes à des programmes gouvernementaux (consulter l’annexe A, *Politique sur la protection de la vie privée*).

atteinte importante à la vie privée

Une atteinte à la vie privée susceptible de créer un risque réel de préjudice important pour une personne. Les préjudices importants comprennent les dommages corporels, l’humiliation, l’atteinte à la réputation ou aux relations, la perte d’emploi, d’affaires ou de possibilités professionnelles, la perte financière, l’usurpation d’identité, les effets négatifs sur le dossier de crédit et l’endommagement ou la perte de biens (consulter l’annexe A, *Politique sur la protection de la vie privée*).

à des fins non administratives

L’utilisation de renseignements personnels dans un but qui n’est pas lié à un processus de prise de décisions touchant directement la personne. Cela comprend l’utilisation de renseignements personnels à des fins de recherche, de statistiques, d’audit et d’évaluation (consulter l’annexe A, *Politique sur la protection de la vie privée*).

renseignements personnels

Information concernant une personne identifiable, enregistrée sous quelque forme que ce soit (consulter l’article 3, *Loi sur la protection des renseignements personnels*).

protocole régissant l’utilisation des renseignements personnels

Ensemble de procédures documentées à suivre lors de l’utilisation de renseignements personnels à des fins non administratives, notamment à des fins de recherche, de statistiques, d’audit et d’évaluation. Ces procédures visent à garantir que les renseignements personnels de la

personne sont traités d'une façon qui est conforme aux principes de la loi (consulter l'annexe A, *Politique sur la protection de la vie privée*).

renseignements accessibles au public

Les renseignements qui ont été publiés ou diffusés pour le public, qui sont accessibles au public sur l'infrastructure mondiale des renseignements ou autrement, ou qui sont mis à la disposition du public sur demande, par abonnement ou par achat. Ils ne comprennent pas les renseignements pour lesquels un Canadien, une Canadienne ou une personne au Canada peut raisonnablement s'attendre à ce que sa vie privée soit respectée. (Extrait de la *Loi sur le Centre de la sécurité des télécommunications*).

---

1 Consulter l'annexe A, Q4, Avis de mise en œuvre de la protection des renseignements personnels 2021-01 : Exigences en matière de protection de la vie privée dans les comptes de médias sociaux officiels

2 Par exemple, l'utilisation de fournisseurs tiers disposant d'une interface de programmation d'applications (API) pour accéder aux plateformes de médias sociaux, ou de moissonnage du Web pour recueillir des renseignements directement à partir de sites Web ou de plateformes de médias sociaux.

3 L'utilisation des renseignements personnels de personnes pour créer un compte non attribuable pourrait constituer une violation des articles 366 et 403 du *Code criminel*.

ISBN: 978-0-660-67780-4

Date de modification :

2023-09-05