Directive sur les pratiques relatives à la protection de la vie privée

Publié : le 2024-03-04

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

No de catalogue BT39-10/2024F-PDF
ISBN: 978-0-660-71386-1

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: Directive on Privacy Practices

Directive sur les pratiques relatives à la protection de la vie privée

1. Date d'entrée en vigueur

1.1 La présente directive entre en vigueur le 26 octobre, 2022.

1.2 La présente directive remplace la *Directive sur les pratiques relatives à la protection de la vie privée* datée du 6 mai 2014.

2. Pouvoirs

2.1 La présente directive est émise en vertu de l'alinéa 71(1)*d)* de *la Loi sur la protection des renseignements personnels* (la *Loi*) et conformément à la section 2.2 de la *Politique sur la protection de la vie privée.*

3. Objectifs et résultats escomptés

3.1 En plus des objectifs précisés dans la section 3.1 de la *Politique sur la protection de la vie privée*, les objectifs de la présente directive consistent à faciliter la mise en œuvre et la publication de pratiques solides et uniformes de gestion de la vie privée pour la protection des renseignements personnels tout au long de leur cycle de vie, qui comprend la création, la collecte, la conservation, l'usage, la communication et le retrait des renseignements personnels relevant des institutions fédérales, que les renseignements soient détenus par l'institution ou par un tiers agissant dans le cadre d'un accord d'échange de renseignements, d'une entente d'échange de renseignements ou d'un contrat avec une institution fédérale.

3.2 Les résultats escomptés de la présente directive sont les suivants :

3.2.1 Les renseignements personnels sont toujours crées, recueillis, conservés, utilisés, communiqués et détruits d'une manière qui respecte la vie privée des individus et les dispositions de la *Loi* et du *Règlement sur la protection des renseignements personnels* (le *Règlement*).

3.2.2 Les fichiers de renseignements personnels (FRP) et les catégories de renseignements personnels des institutions fédérales sont décrits d'une manière qui facilite pour les individus le processus de demande d'accès à leurs renseignements personnels et de correction de leurs renseignements personnels.

3.2.3 Les fins pour lesquelles les institutions fédérales recueillent les renseignements personnels et les pratiques relatives à la protection de la vie privée qui appuient l'administration des programmes et des activités sont décrites dans les FRP et les catégories de renseignements personnels.

3.2.4 Les atteintes à la vie privée sont gérées efficacement et des mesures préventives appropriées sont en place.

3.2.5 Les renseignements personnels relevant des institutions fédérales sont exacts.

4. Exigences

4.1 Les responsables des institutions fédérales ou leurs délégués assument les responsabilités suivantes :

4.1.1 Établir des pratiques efficaces de protection de la vie privée au sein de leur institution comme il est énoncé ci-après. Les fonctionnaires ou les employés doivent respecter ces pratiques lorsqu'ils participent à des activités liées à la création, la collecte, la conservation, l'usage, l'exactitude, la communication ou le retrait de renseignements personnels qui relèvent de l'institution fédérale, y compris les renseignements personnels des fonctionnaires ou des employés de l'institution fédérale tels que définis par la *Loi*.

Formation sur la protection des renseignements personnels

4.1.2 Veiller à ce que les employés des institutions fédérales reçoivent une formation sur la protection des renseignements personnels telle qu'énoncée à l'annexe B de la *Directive sur les demandes de renseignements personnels et de correction des renseignements personnels*.

4.1.3 Documenter l'achèvement de la formation conformément à l'annexe B de la *Directive sur les demandes de renseignements personnels et de correction de renseignements personnels*.

Atteintes à la vie privée

4.1.4 Veiller à ce que les plans visant à répondre aux atteintes à la vie privée qui touchent les renseignements personnels relevant de l'institution, y compris celles qui se produisent au sein des entités tierces ou qui sont causées par des entités tierces, satisfassent aux exigences suivantes :

4.1.4.1 les rôles et les responsabilités en cas d'atteinte à la vie privée sont définis clairement;

4.1.4.2 les procédures et les communications internes sont conformes à la *Politique sur la sécurité du gouvernement* et à ses directives et normes

connexes; et

4.1.4.3 les exigences énoncées à l’annexe B : Procédures obligatoires pour les atteintes à la vie privée sont respectées.

4.1.5 En cas d’atteinte à la vie privée qui touche des renseignements personnels qui sont détenus par l’institution mais qui relèvent d’une autre institution, en aviser rapidement l’institution dont les renseignements personnels relèvent et, au besoin, entreprendre des démarches correctives en coordination avec l’institution pour s’assurer que les exigences énoncées à l’annexe B : Procédures obligatoires pour les atteintes à la vie privée sont respectées.

4.1.6 Exécuter les procédures obligatoires requises des responsables des institutions fédérales ou de leurs délégués énoncées à l’annexe B : Procédures obligatoires pour les atteintes à la vie privée.

Fichiers de renseignements personnels et catégories de renseignements personnels

4.1.7 S’assurer que le processus de création des FRP, nouveaux ou ayant subi des modifications importantes, est conforme au processus de création et d’approbation de l’évaluation des facteurs relatifs à la vie privée de base comme l’exige la *Directive sur l’évaluation des facteurs relatifs à la vie privée*.

4.1.8 Présenter au Secrétariat du Conseil du Trésor (SCT) une demande d’enregistrement de tout nouveau FRP ou d’élimination d’un FRP existant.

4.1.9 Veiller à ce que les demandes d’enregistrement des FRP comprennent tous les éléments du FRP indiqués aux sous-alinéas 11(1)a)(i) jusqu’à (vi) de la *Loi*, accompagnés d’une évaluation des facteurs relatifs à la vie privée de base complète et approuvée.

4.1.10 Veiller à ce que les demandes d’élimination d’un FRP comprennent :

4.1.10.1 une explication justifiant l’élimination du FRP; et

4.1.10.2 la confirmation que les dossiers et les renseignements personnels qu’ils contiennent ont été détruits conformément à l’Autorisation de disposer de documents de l’institution et ne relèvent plus de l’institution fédérale.

4.1.11 Veiller au respect des exigences énoncées à l’annexe C : Exigences supplémentaires en vertu de la *Loi sur la protection des renseignements personnels* pour les ministères au sens de l’article 2 de la *Loi sur la gestion des finances publiques* pour les approbations par le président du Conseil du Trésor dans le cas des FRP, à moins que le pouvoir d’approbation ait été délégué au responsable de l’institution par le président du Conseil du Trésor, sous réserve des modalités en place.

4.1.12 Informer le SCT des changements aux FRP.

4.1.13 Veiller à ce que le SCT reçoive une évaluation des facteurs relatifs à la vie privée de base lorsque les changements aux FRP sont importants, comme l'exige la *Directive sur l'évaluation des facteurs relatifs à la vie privée*.

4.1.14 Mettre à jour le répertoire prescrit des descriptions de FRP, Info Source, pour tous les FRP nouveaux, modifiés ou éliminés et pour tout changement aux catégories de renseignements personnels.

Fichiers inconsultables

4.1.15 Veiller à ce que les propositions soumises au SCT visant la constitution ou l'élimination d'un fichier inconsultable contiennent :

4.1.15.1 une description des renseignements qui seront inclus dans le fichier inconsultable, ainsi qu'une explication justifiant pourquoi les renseignements devraient être inclus dans un fichier inconsultable;

4.1.15.2 la confirmation que les dossiers dans le fichier se composent principalement de renseignements personnels comme il est décrit à l'article 21 ou 22 de la *Loi*;

4.1.15.3 la disposition de l'exception spécifique de la *Loi* sur laquelle on s'appuie;

4.1.15.4 l'énoncé des effets préjudiciables envisagés pour toute exception fondée sur critère subjectif; et

4.1.15.5 l'ébauche du décret et l'ébauche du Résumé de l'étude d'impact de la réglementation.

Demandes et communications à des organismes d'enquête

4.1.16 Se conformer aux exigences concernant les demandes présentées par les organismes d'enquête et les communications faites aux organismes d'enquête énoncés à l'annexe D : Exigences relatives à l'alinéa 8(2)e) de la *Loi sur la protection des renseignements personnels*.

Documentation relative aux nouveaux usages et communications

4.1.17 Établir des procédures pour assurer la tenue d'un relevé des nouveaux usages et communications, ainsi que tout usage compatible qui n'est pas décrit dans un FRP. Ces procédures permettront de veiller à ce que :

4.1.17.1 les descriptions d'usage, de communication et des fins de la collecte que l'on consigne dans les FRP soient tenues à jour (cette exigence ne s'applique pas aux communications faites aux organismes d'enquête);

4.1.17.2 tout nouvel usage compatible soit indiqué dans les FRP pertinents;

4.1.17.3 le Commissaire à la protection de la vie privée du Canada soit avisé de tout nouvel usage compatible.

Web analytique et protection de la vie privée

4.1.18 Veiller à ce que l'on utilise des outils du Web analytique pour mesurer et améliorer le rendement des sites Web du gouvernement du Canada en conformité avec l'annexe E : Norme sur la protection de la vie privée en matière de Web analytique.

Surveillance et établissement de rapports

4.1.19 Surveiller les exigences de la présente directive conformément à la *Politique sur la protection de la vie privée* et établir des rapports à ce sujet.

4.2 Les cadres et les agents principaux qui gèrent des programmes ou des activités comportant la création, la collecte ou le traitement de renseignements personnels assument les responsabilités suivantes :

Pratiques relatives à la protection de la vie privée

4.2.1 Informer le responsable de l'institution fédérale ou son délégué de tout nouveau programme ou toute nouvelle activité, ou toute modification importante apportée à une activité ou à un programme existant, dans le cas où les renseignements personnels d'un individu sont recueillis ou traités dans le cadre d'un processus décisionnel exerçant une incidence directe sur la personne concernée.

4.2.2 S'assurer que les pratiques de protection de la vie privée sont conformes et adhèrent aux dispositions figurant dans la *Loi*, le *Règlement* et toute autre loi applicable, y compris la loi habilitante de l'institution fédérale.

4.2.3 Informer les employés des conséquences légales et administratives de l'accès inapproprié ou non autorisé aux renseignements personnels ou de l'usage, la communication, la modification, la conservation ou le retrait inapproprié ou non autorisé des renseignements personnels, dans le cadre d'une activité ou d'un programme particulier.

Atteintes à la vie privée

4.2.4 Mettre en œuvre les plans de l'institution visant à répondre aux atteintes à la vie privée.

4.2.5 Veiller à ce que le responsable de l'institution fédérale ou son délégué soit avisé de toute atteinte potentielle ou confirmée à la vie privée qui touche des renseignements

personnels détenus par l'institution ou qui relèvent de l'institution, y compris tout cas qui se produit au sein d'un tiers.

4.2.6 Exécuter les procédures obligatoires requises des cadres et des agents principaux qui gèrent des programmes ou des activités comportant la création, la collecte ou le traitement de renseignements personnels énoncés à l'annexe B : Procédures obligatoires pour les atteintes à la vie privée.

Collecte et création de renseignements personnels

4.2.7 S'assurer, avant la collecte des renseignements personnels, que l'institution a l'autorité légitime pour le programme ou l'activité pour lequel les renseignements personnels sont recueillis. L'obtention du consentement d'un individu pour recueillir ses renseignements personnels ne remplace ni n'établit l'autorité légitime pour recueillir ces renseignements personnels.

4.2.8 Déterminer les éléments à inclure dans le FRP avant toute nouvelle collecte de renseignements personnels.

4.2.9 Limiter la collecte de renseignements personnels à ceux qui sont directement liés et manifestement nécessaires aux programmes ou aux activités de l'institution fédérale. La création de renseignements personnels par l'institution fédérale constitue également une collecte en vertu de la *Loi*.

Avis de confidentialité

4.2.10 Aviser l'individu, dont les renseignements personnels font l'objet d'une collecte directe, des éléments suivants :

- 4.2.10.1 les fins de la collecte et en vertu de quelle autorité légitime elle est faite;
- 4.2.10.2 tout usage ou communication compatible avec la fin originale;
- 4.2.10.3 toute conséquence administrative ou légale découlant d'un refus de fournir les renseignements personnels;
- 4.2.10.4 la description du FRP associée;
- 4.2.10.5 les droits d'accès, de correction et de protection des renseignements personnels en vertu de la *Loi*; et
- 4.2.10.6 le droit de déposer une plainte auprès du Commissaire à la protection de la vie privée du Canada concernant le traitement des renseignements personnels des individus par l'institution.

4.2.11 Adapter l'avis de confidentialité, au moment de la collecte, aux fins de communication écrite ou orale.

Consentement au sujet de la collecte, de l’usage et de la communication

4.2.12 Obtenir le consentement d’un individu pour les fins suivantes :

4.2.12.1 collecte indirecte de renseignements personnels, sauf en cas de collecte à des fins non administratives ou à des fins énumérées au paragraphe 8(2) de la *Loi*, ou si la demande d’un consentement risquerait soit d’entraîner la collecte de renseignements inexacts, soit de contrarier les fins ou de compromettre l’usage auxquels les renseignements sont destinés;

4.2.12.2 usage ou communication ne respectant pas les fins pour lesquelles les renseignements ont été recueillis ou préparés, sauf si l’usage ou la communication est autorisé en vertu du paragraphe 8(2) de la *Loi*;

4.2.12.3 tout retrait de renseignements personnels avant la fin de la période minimale de conservation de deux ans stipulée par le *Règlement* à moins qu’un tel retrait ne soit expressément autorisé par la *Loi*.

4.2.13 Inclure, le cas échéant, les éléments suivants dans la demande de consentement :

4.2.13.1 la fin pour laquelle le consentement est demandé;

4.2.13.2 les éléments de renseignements personnels demandés;

4.2.13.3 dans le cas d’une collecte indirecte, les sources qui seront sollicitées pour fournir les renseignements et la justification d’une telle collecte;

4.2.13.4 les usages et les communications non compatibles avec les fins pour lesquelles les renseignements ont été recueillis et pour lesquelles un consentement est demandé;

4.2.13.5 toute conséquence pouvant résulter d’un refus d’accorder le consentement; et

4.2.13.6 toute alternative à donner son consentement.

4.2.14 S’assurer que le consentement est obtenu par écrit ou qu’il est autrement documenté adéquatement, y compris la date et l’heure du consentement.

Exactitude

4.2.15 Prendre toutes les mesures raisonnables pour s’assurer que les renseignements personnels utilisés dans un processus décisionnel sont autant que possible exacts, à jour et complets. Cela comprend recueillir les renseignements personnels directement de l’individu, chaque fois que possible, sauf en cas d’autorisation contraire de l’individu ou pour des raisons mentionnées au paragraphe 5(1) de la *Loi*.

4.2.16 Dans les cas où les renseignements personnels sont recueillis indirectement sans que le consentement soit obtenu, mettre en œuvre des mesures pour :

4.2.16.1 s’assurer que les renseignements personnels sont obtenus d’une source fiable;

4.2.16.2 vérifier ou valider l’exactitude des renseignements personnels avant de les utiliser.

4.2.17 Lors de la validation de l’exactitude des renseignements personnels, documenter la source ou la technique utilisée pour valider les renseignements personnels.

4.2.18 Lors de la validation de l’exactitude des renseignements personnels, indiquer dans la description du FRP pertinent la source ou la technique utilisée, y compris tout couplage de données, lorsque cela est approprié.

4.2.19 S’assurer que les individus ont, dans la mesure du possible, la possibilité de corriger tout renseignement personnel inexact les concernant avant la prise de toute décision qui pourrait avoir une incidence sur eux.

Mesures de protection relatives à la collecte, l’usage et la communication

4.2.20 Limiter l’accès aux renseignements personnels aux personnes qui occupent des postes ou des fonctions dans le cadre du programme ou de l’activité et qui ont une raison valable d’accéder aux renseignements personnels.

4.2.21 Limiter l’accès aux renseignements personnels, leur usage et leur communication par des mesures administratives, physiques et techniques, de manière à protéger ces renseignements.

4.2.22 Prendre des mesures appropriées pour s’assurer que l’accès aux renseignements personnels, ainsi que leur usage et leur communication sont surveillés et documentés, afin de pouvoir identifier en temps opportun les atteintes à la vie privée.

Contrats, accords et ententes

4.2.23 Établir un contrat, un accord d’échange de renseignements ou une entente d’échange de renseignements comportant des mesures de protection appropriées avant que les renseignements personnels ne soient communiqués à un autre programme fédéral ou à une autre entité du secteur public ou privé, à moins que les renseignements personnels soient échangés en vertu d’un traité international conformément aux normes internationales.

4.2.24 S’assurer que les mesures de protection appropriées, pour les contrats, les accords d’échange de renseignements et les ententes d’échange de renseignements assujettis à 4.2.23 qui entrent en vigueur ou sont modifiés de façon substantielle

après la date d'entrée en vigueur de la présente directive, comprennent des dispositions qui portent sur les éléments suivants :

4.2.24.1 les éléments de renseignements personnels précis qui seront communiqués;

4.2.24.2 la fin précise ou les fins précises de la communication;

4.2.24.3 les restrictions régissant la collecte, l'usage et la communication ultérieure des renseignements personnels;

4.2.24.4 la disposition et le retrait adéquats des renseignements personnels, s'il y a lieu, y compris une confirmation de destruction lorsque la destruction est exigée;

4.2.24.5 les mesures de protection administratives, techniques et physiques;

4.2.24.6 l'exigence que tout renseignement personnel communiqué à l'entité ou recueilli par l'entité en vertu du contrat, de l'accord d'échange de renseignements ou de l'entente d'échange de renseignements relèvent de l'institution fédérale de manière continue;

4.2.24.7 l'obligation de se coordonner avec l'institution fédérale de manière que l'institution puisse s'acquitter de ses obligations en vertu de la section 12 de la *Loi sur la protection des renseignements personnels* concernant le droit d'accès d'un individu.

4.2.24.8 pour les institutions fédérales qui sont assujetties à la *Politique sur la sécurité du gouvernement*, l'obligation de suivre toute orientation émise par les principaux organismes chargés de la sécurité, comme il est énoncé à la section 5 de cette politique;

4.2.24.9 la déclaration obligatoire à l'institution fédérale en temps opportun de toute atteinte potentielle ou confirmée à la vie privée qui touche les renseignements personnels;

4.2.24.10 pour les entités non assujetties à la *Loi sur la protection des renseignements personnels*,l'obligation en cas d'atteinte potentielle ou confirmée à la vie privée de fournir à l'institution fédérale qui dirige l'enquête, sur demande, un accès suffisant aux fonds de renseignements personnels pour mener une évaluation de l'atteinte potentielle ou confirmée; et

4.2.24.11 un examen obligatoire du contrat, de l'accord d'échange de renseignements ou de l'entente d'échange de renseignements, à un intervalle convenu par les parties.

4.2.25 Mettre le contrat, l'accord d'échange de renseignements ou l'entente d'échange de renseignements assujetti à 4.2.23 à la disposition du Commissariat à la protection de

la vie privée et du SCT sur demande.

4.2.26 Mettre à la disposition du public, par le biais de la mise à jour annuelle d'Info Source de l'institution, un résumé du contrat, de l'accord d'échange de renseignements ou de l'entente d'échange de renseignements assujetti à 4.2.23, sauf en cas de communication unique.

4.2.27 Respecter les exigences en matière de sécurité ainsi que toute autre considération juridique ou de confidentialité lorsque l'on met un résumé d'un contrat, d'un accord d'échange de renseignements ou d'une entente d'échange de renseignements à la disposition du public.

Cession ou privatisation

4.2.28 Dans le cas où des renseignements personnels sont transférés hors de l'autorité d'une institution fédérale à la suite de la cession ou de la privatisation d'un programme ou d'une activité, s'assurer que :

4.2.28.1 l'autorisation pour le transfert est établie;

4.2.28.2 des pratiques adéquates relatives à la protection des renseignements personnels sont en place avant le transfert;

4.2.28.3 les droits d'accès des individus à leurs renseignements personnels et leurs droits de correction de ces renseignements seront maintenus après le transfert;

4.2.28.4 un accord de transfert de documents, respectant toute autorisation de disposer de documents existante, est conclu pour établir les modalités relatives aux documents faisant l'objet du transfert;

4.2.28.5 le consentement du bibliothécaire et archiviste du Canada est obtenu avant le transfert des documents; et

4.2.28.6 un avis de la cession ou de la privatisation est mis à la disposition du public par le biais de la mise à jour annuelle d'Info Source de l'institution.

Documentation de communications et d'usages nouveaux

4.2.29 Aviser le responsable de l'institution fédérale ou le délégué approprié de tout usage, fin ou communication de renseignements personnels dont il n'est pas fait mention dans la description du FRP et veiller à ce que le FRP soit mise à jour en conséquence.

Conservation et retrait de renseignements personnels

4.2.30 Appliquer les normes de conservation des renseignements personnels de l'institution ainsi que les autorisations de disposition établies par Bibliothèque et Archives Canada et les indiquer dans le FRP pertinent.

4.2.31 S'assurer que les renseignements personnels d'un individu qui ont servi à des fins administratives sont conservés par l'institution conformément au paragraphe 6(1) de la *Loi* et aux alinéas 4(1)a) et b) du *Règlement*.

4.2.32 Examiner régulièrement les dossiers décrits dans les FRP, y compris ceux des fichiers inconsultables, et détruire les documents renfermant des renseignements personnels conformément aux directions fournies par Bibliothèque et Archives Canada, comme il est stipulé aux articles 12 à 14 de la *Loi sur la Bibliothèque et les Archives du Canada*.

4.2.33 Lorsque l'institution est assujettie à la *Politique sur la sécurité du gouvernement*, détruire les documents en respectant les normes de sécurité gouvernementales.

Web analytique et protection de la vie privée

4.2.34 Informer les employés et toute autre personne responsable de la gestion des sites Web de l'institution, ainsi que les spécialistes fonctionnels et les propriétaires de contenu Web, de la nécessité de se conformer aux exigences de l'annexe E : Norme sur la protection de la vie privée en matière de Web analytique.

4.3 Les employés des institutions fédérales assument les responsabilités suivantes :

Atteintes à la vie privée

4.3.1 Exécuter les procédures obligatoires requises des employés énoncées à l'annexe B : Procédures obligatoires pour les atteintes à la vie privée.

Web analytique et protection de la vie privée

4.3.2 Effectuer une analytique Web, si autorisé à le faire, conformément aux exigences de l'annexe E : Norme sur la protection de la vie privée en matière de Web analytique.

Formation sur la protection des renseignements personnels

4.3.3 Suivre une formation sur la protection des renseignements personnels telle qu'énoncée à l'annexe B de la *Directive sur les demandes de renseignements personnels et de correction des renseignements personnels*.

5. Rôles des autres organisations gouvernementales

5.1 Cette section décrit les rôles des autres organisations gouvernementales clés au regard de la présente directive. En soi, cette section ne confère aucun pouvoir.

5.2 Le SCT est chargé d'appuyer le président du Conseil du Trésor dans l'exercice des fonctions suivantes :

5.2.1 établir les modalités d'approbation des FRP, ainsi que les modalités de délégation de ce pouvoir d'approbation aux responsables des ministères;

5.2.2 révoquer tout décret de délégation de pouvoir délivrée aux termes du paragraphe 71(6) de la *Loi* en cas de problème systémique de conformité au sein d'une institution fédérale.

5.2.3 surveiller et suivre les atteintes substantielles à la vie privée dans l'ensemble du gouvernement.

5.3 Le Bureau du dirigeant principal de l'information du SCT est chargé d'approuver les techniques de dépersonnalisation qu'un fournisseur de services tiers est tenu d'utiliser en vertu de la sous-section E.2.2.3 de l'annexe E : Norme sur la protection de la vie privée en matière de Web analytique aux fins de l'analytique Web sur les serveurs hébergés à l'externe par le tiers.

6. Application

6.1 La présente directive s'applique tel que décrit à la section 6 de la *Politique sur la protection de la vie privée*.

7. Références

7.1 Textes législatifs

- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la gestion des finances publiques*
- *Loi sur la protection des renseignements personnels*
- *Loi sur Services partagés Canada*
- *Règlement sur la protection des renseignements personnels*

7.2 Instruments de politique connexes

- *Directive sur les services et le numérique*
- *Directive sur l'évaluation des facteurs relatifs à la vie privée*
- *Politique sur la protection de la vie privée*
- *Politique sur la sécurité du gouvernement*

7.3 Instruments d'orientation connexes

- Avis de mise en œuvre sur l’accès à l’information et la protection des renseignements personnels
- Document d’orientation pour aider à préparer des Ententes d’échange de renseignements personnels
- Document d’orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché
- Ligne directrice sur les services et le numérique
- Trousse d’outils pour la gestion des atteintes à la vie privée

8. Demandes de renseignements

8.1 Le public peut communiquer avec le service de demandes de renseignements du Secrétariat du Conseil du Trésor du Canada pour toute question concernant cette directive.

8.2 Les employés des institutions fédérales peuvent communiquer avec leur coordonnateur de l’accès à l’information et de la protection des renseignements personnels pour toute question concernant cette directive.

8.3 Les coordonnateurs de l’accès à l’information et de la protection des renseignements personnels peuvent communiquer avec la Division de la protection de la vie privée et des données du Secrétariat du Conseil du Trésor du Canada pour toute question concernant cette directive.

Annexe A : Définitions

A.1 Aux fins de l’interprétation de la présente directive, les définitions énumérées ci-dessous, en plus des définitions énumérées à l’annexe A de la *Politique sur la protection de la vie privée*, doivent être utilisées.

accord d’échange de renseignements (*information sharing agreement*)
Une entente écrite qui décrit les modalités sous lesquelles des renseignements personnels sont communiqués entre parties. Un accord d’échange de renseignements est généralement utilisé pour faciliter la communication de renseignements personnels d’une institution fédérale à une entité du secteur public extérieure à la Couronne. Un accord d’échange de renseignements peut être ou ne pas être juridiquement contraignant.

adresse du protocole Internet (IP) (*Internet Protocol address*)
Étiquette numérique attribuée par le fournisseur de services Internet à chaque ordinateur. Il s’agit de la façon dont l’utilisateur de l’ordinateur communique sur Internet. Une adresse IP peut, dans certaines circonstances, être associée à un individu identifiable dont l’ordinateur utilise cette adresse à tout moment. Pour cette raison, le gouvernement du Canada considère l’adresse IP comme étant un renseignement personnel qui doit, dans tous les cas, être traité conformément aux exigences de la *Loi*.

avis de confidentialité (*privacy notice*)

Avis verbal ou écrit présenté à un individu afin de communiquer les fins de la collecte de leurs renseignements personnels ainsi que l'autorité légitime de l'institution fédérale pour procéder à cette collecte. L'avis, qui doit renvoyer au FRP décrit dans l'Info Source, informe également l'individu de la façon dont ses renseignements personnels seront utilisés et communiqués, de ses droits d'accès et de correction de ses renseignements personnels, des conséquences d'un refus de fournir les renseignements demandés, ainsi que de son droit de déposer une plainte auprès du Commissaire à la protection de la vie privée du Canada.

catégories de renseignements personnels (*classes of personal information*)

Des descriptions de renseignements personnels qui relèvent de l'institution fédérale mais dont on ne prévoit pas faire usage pour des fins administratives ou que l'on ne peut pas retrouver par référence au nom d'un individu ou à une indication identificatrice propre à cet individu (p. ex. opinions non sollicitées et correspondance générale). Les catégories de renseignements personnels doivent être énumérées et décrites dans l'Info Source de l'institution.

collecte directe (*direct collection*)

Collecte de renseignements personnels auprès de l'individu concerné.

collecte indirecte (*indirect collection*)

Collecte de renseignements personnels auprès d'une source autre que l'individu concerné.

création de renseignements personnels (*creation of personal information*)

Tout élément ou sous-élément de renseignements personnels qu'une institution fédérale attribue à un individu identifiable sans égard au fait que les renseignements proviennent de renseignements personnels existants relevant de l'institution fédérale ou que l'institution fédérale ajoute de nouveaux renseignements au fichier de l'individu. La création de renseignements personnels est considérée une collecte en vertu de la *Loi sur la protection des renseignements personnels*.

entente d'échange de renseignements (*information sharing arrangement*)

Une entente écrite qui décrit les modalités sous lesquelles des renseignements personnels sont communiqués entre parties. Une entente d'échange de renseignements est généralement utilisée pour faciliter la communication de renseignements personnels entre institutions fédérales et au sein de celles-ci. Une entente d'échange de renseignements n'est pas juridiquement contraignante.

fin originale (*original purpose*)

La fin initiale identifiée lors de la collecte des renseignements personnels qui est liée directement à un programme ou à une activité d'ordre opérationnel de l'institution. Une fin qui ne correspond pas à la fin originale est traitée comme étant une fin secondaire.

fournisseur de services Internet (*internet service provider*)

Organisation qui fournit un accès à Internet.

marqueurs numériques (*digital markers*)

Outils de suivi utilisés pour garder en mémoire les interactions en ligne du visiteur avec des sites Web. Ces outils peuvent enregistrer les interactions en ligne d'un visiteur lors d'une session ou visite unique, ou peuvent enregistrer les interactions en ligne d'un visiteur lors de multiples sessions ou visites.

mesures de protection administrative (*administrative safeguards*)

Politiques, directives, règles, procédures et processus qui visent la protection des renseignements personnels tout au long du cycle de vie tant des renseignements personnels que du programme ou de l'activité (p. ex. politique sur la sécurité de l'institution, dispositions de sécurité dans un contrat de service pour assurer la destruction des documents).

mesures de protection physique (*physical safeguards*)

Installations et équipement qui servent à protéger les renseignements personnels (p. ex. locaux de rangement fermés à clé, classeurs fermés à clés).

mesures de protection technique (*technical safeguards*)

Mesures de la technologie de l'information utilisées pour protéger les installations, l'équipement et le système de soutien où les renseignements personnels sont enregistrés et conservés (p. ex. dispositifs de contrôle d'accès électroniques, contrôles de vérification).

pratiques relatives à protection de la vie privée (*privacy practices*)

Toutes les pratiques relatives à la création, la collecte, la conservation, l'exactitude, la correction, l'usage, la communication et le retrait des renseignements personnels.

principalement (*predominantly*)

Dans le contexte d'un fichier inconsultable, ce terme signifie que plus de la moitié de l'information de chaque dossier contenu dans le fichier peut faire l'objet d'une exception en vertu de l'article 21 ou 22 de la *Loi*.

résumé de l'étude d'impact de la réglementation (REIR) (*Regulatory Impact Analysis Statement (RIAS)*)

Outil utilisé dans le cadre d'un changement réglementaire afin d'en évaluer l'impact sur l'environnement, la santé, la sécurité et le bien-être social et économique des Canadiens.

source fiable (*reliable source*)

Source de renseignements ou fonds de données que l'on considère être exacts et à jour. Il est possible de faire confiance à une telle source lorsqu'il s'agit de recueillir ou de valider des renseignements personnels.

témoins internes (de premier niveau) (*first-party cookie*)

Un témoin est un fichier de données envoyé par un serveur Web au navigateur Web qui se trouve sur l'ordinateur d'un visiteur et que le serveur Web utilise pour faire le suivi ou enregistrer les renseignements sur le visiteur. Un témoin interne (de premier niveau) est celui qui est créé par le site Web que le visiteur consulte.

traitement (*handling*)

Tout processus visant des renseignements personnels, y compris la collecte, la correction, la création, la modification, l'usage, la conservation, la communication et le retrait.

Web analytique (*web analytics*)

La collecte, l'analyse, la mesure et le compte rendu des données sur l'achalandage des sites Web et les visites d'utilisateurs pour bien comprendre l'usage du Web et l'optimaliser.

Annexe B : Procédures obligatoires pour les atteintes à la vie privée

B.1 Date d'entrée en vigueur

B.1.1 Ces procédures obligatoires entrent en vigueur le 1 mars, 2024.

B.1.2 Ces procédures obligatoire remplacent l'annexe B : Procédures obligatoires pour les atteintes à la vie privée datée du octobre 26, 2022.

B.2 Procédures

B.2.1 Ces procédures obligatoires pour les atteintes à la vie privée contiennent des détails sur les exigences énoncées à la section 4 de la *Directive sur les pratiques relatives à la protection de la vie privée*.

B.2.2 Les employés des institutions fédérales doivent :

B.2.2.1 Prendre des mesures immédiates pour limiter toute atteinte potentielle ou confirmée à la vie privée et protéger les renseignements personnels concernés.

B.2.2.2 Une fois que toutes mesures pour limiter une atteinte potentielle ou confirmée à la vie privée ont été prises, en aviser immédiatement le responsable de l'institution ou son délégué. L'avis doit comprendre :

B.2.2.2.1 la date, l'heure et le lieu de l'atteinte potentielle ou confirmée à la vie privée; et

B.2.2.2.2 une brève description de l'atteinte potentielle ou confirmée à la vie privée, y compris le type de renseignements personnels en cause et le nombre de personnes potentiellement touchées, ainsi que les mesures prises pour limiter l'atteinte potentielle ou confirmée.

B.2.3 Les cadres et les agents principaux qui gèrent des programmes ou des activités comportant la création, la collecte ou le traitement de renseignements personnels doivent prendre les mesures suivantes :

B.2.3.1 Si les renseignements personnels touchés par une atteinte à la vie privée font l'objet d'un contrat, d'un accord d'échange de renseignements ou d'une entente d'échange de renseignements, en aviser rapidement les parties au contrat, à l'accord ou à l'entente.

B.2.3.2 S'il est déterminé par le responsable de l'institution fédérale ou son délégué qu'une évaluation complète d'une atteinte est nécessaire, veiller à ce qu'un agent de programme approprié soit affecté à la coordination avec le responsable de l'institution fédérale ou son délégué.

B.2.3.3 En coordination avec le responsable de l'institution fédérale ou son délégué, déterminer les mesures d'atténuation appropriées afin de réduire le risque de préjudice pour les individus touchés et pour l'institution qui découle de l'atteinte, qui doivent comprendre un avis aux personnes touchées dans le cas d'une atteinte substantielle à la vie privée, à moins qu'un tel avis soit inapproprié pour des raisons de sécurité, de confidentialité, juridiques ou autres.

B.2.3.4 En coordination avec le responsable de l'institution fédérale ou son délégué, déterminer les mesures de prévention appropriées pour réduire le risque d'atteintes futures.

B.2.3.5 Mettre en œuvre les mesures d'atténuation et de prévention déterminées comme étant appropriées dans un délai raisonnable.

B.2.4 Les responsables des institutions fédérales ou leurs délégués doivent :

B.2.4.1 Après avoir reçu un avis d'une atteinte à la vie privée potentielle, vérifier s'il s'agit réellement d'une atteinte à la vie privée.

B.2.4.2 En cas d'atteinte à la vie privée, déterminer la nécessité d'une évaluation complète. Une évaluation complète détermine et documente, au minimum :

B.2.4.2.1 les circonstances ayant donné lieu à l'atteinte;

B.2.4.2.2 l'inventaire des renseignements personnels touchés;

B.2.4.2.3 les personnes dont les renseignements personnels ont été touchés;

B.2.4.2.4 les secteurs institutionnels et les tiers, le cas échéant, ayant un rôle direct ou indirect dans le traitement des renseignements personnels en cause;

B.2.4.2.5 le risque de préjudice pour les individus touchés et pour l'institution; et

B.2.4.2.6 si l'atteinte constitue une atteinte substantielle à la vie privée.

B.2.4.3 Collaborer au besoin avec les responsables de la sécurité du ministère, y compris ceux qui sont chargés de la cybersécurité le cas échéant, pour toute évaluation de l'atteinte à la vie privée ou enquête sur un événement de sécurité connexe.

B.2.4.4 Inclure, au minimum et lorsqu'ils sont connus, les renseignements suivants au moment de signaler une atteinte substantielle à la vie privée au Commissariat à la protection de la vie privée et au SCT :

B.2.4.4.1 la date de l'atteinte ou la période où l'atteinte s'est produite; et la date à laquelle l'institution a découvert l'atteinte

B.2.4.4.2 une description de l'atteinte, y compris le type et la cause;

B.2.4.4.3 le nombre de personnes touchées ou une approximation de ce nombre;

B.2.4.4.4 les catégories et les éléments de renseignements personnels en cause;

B.2.4.4.5 les parties en cause, incluant la catégorie de personnes touchées par l'atteinte et les relations entre les parties concernées;

B.2.4.4.6 une description des mesures de protection pertinentes qui étaient en place;

B.2.4.4.7 les risques réels de préjudices graves qui sont prévus;

B.2.4.4.8 toutes les mesures correctives, y compris toutes les mesures pour limiter l'atteinte et toutes les mesures d'atténuation et de prévention, qui ont été ou qui seront prises;

B.2.4.4.9 la méthode utilisée pour aviser les personnes dont les renseignements personnels ont été touchés, le cas échéant;

B.2.4.4.10 une justification au cas où les personnes dont les renseignements personnels ont été touchés ne seraient pas avisées;

B.2.4.4.11 Le lieu physique ou géographique où l'atteinte s'est produite;

B.2.4.4.12 Une description de la manière dont l'atteinte a été découverte;

B.2.4.4.13 Les fichiers de renseignements personnels (FRP) pour les informations faisant l'objet de l'atteinte, si applicable;

B.2.4.4.14 Une liste de toutes les organisations qui ont été notifiées de l'atteinte.

B.2.4.5 Pour signaler une atteinte substantielle à la vie privée au CPVP et au SCT, utilisez le moyen suivant :

B.2.4.5.1 le Formulaire de rapport d'atteintes substantielles à la vie privée en vertu de la *Loi sur la protection de la vie privée*

B.2.4.6 Tenir un registre de toute atteinte à la vie privée pendant une période de cinq ans après la date à laquelle l'institution a eu connaissance de l'atteinte. Le registre doit comprendre au moins :

B.2.4.6.1 la date de l'atteinte ou la période où l'atteinte s'est produite;

B.2.4.6.2 une description générale des circonstances de l'atteinte et de la nature des renseignements en cause;

B.2.4.6.3 l'évaluation complète de l'atteinte, si une évaluation complète a été entreprise; et

B.2.4.6.4 dans le cas d'une atteinte substantielle à la vie privée, le rapport fournit au Commissariat à la protection de la vie privée et au SCT.

Annexe C : Exigences supplémentaires en vertu de la Loi sur la protection des renseignements personnels pour les ministères au sens de l'article 2 de la Loi sur la gestion des finances publiques

C.1 Outre l'obligation d'enregistrer et de publier les FRP, les paragraphes 71(3) et 71(4) de la *Loi sur la protection des renseignements personnels* exigent que le président approuve tout FRP, nouveau ou ayant subi des modifications importantes ou devant être éliminé, présenté par les institutions fédérales définies comme ministères à l'article 2 de la *Loi sur la gestion des finances publiques*.

C.2 À moins que ce pouvoir n'ait été délégué par le président du Conseil du Trésor au responsable du ministère en vertu du paragraphe 71(6) de la *Loi*, le responsable ou son délégué responsable en vertu de l'article 10 de cette *Loi* doit :

C.2.1 présenter au SCT pour approbation toutes les propositions visant la création d'un nouveau FRP ou la modification ou la disposition d'un FRP;

C.2.2 fournir une justification ou une analyse appuyant la proposition. Dans le cas d'une proposition visant à créer ou à effectuer des modifications importantes à un FRP qui comprend la prise de décisions administratives, une évaluation des facteurs relatifs à la vie privée de base doit être effectuée (voir la *Directive sur l'évaluation des facteurs relatifs à la vie privée*).

Annexe D : Exigences relatives à l'alinéa 8(2)e) de la Loi sur la protection des renseignements personnels

D.1 L'alinéa 8(2)e) de la *Loi* stipule que des renseignements personnels peuvent être communiqués à l'un des organismes d'enquête spécifiés dans le *Règlement*, sur demande écrite de l'organisme, en vue d'appliquer une loi du Canada ou d'une province ou d'exécuter une enquête licite. Cette disposition n'accorde pas aux organismes d'enquête le droit d'avoir accès aux renseignements personnels. Elle confie toute décision relative à la communication de ces renseignements à la discrétion de l'institution qui est responsable de ces renseignements, une fois que les critères pertinents ont été respectés.

D.2 Les exigences relatives à l'alinéa 8(2)e) de la *Loi* sont les suivantes :

Demandes de renseignements conformément à l'alinéa 8(2)e)

D.2.1 Les demandes de renseignements faites en vertu de l'alinéa 8(2)e) de la *Loi* doivent être soumises par écrit et doivent comporter les éléments suivants :

D.2.1.1 le nom de l'organisme d'enquête;

D.2.1.2 le nom ou autre identificateur personnel de l'individu visé par la demande;

D.2.1.3 l'objet de la demande et une description des renseignements à communiquer;

D.2.1.4 l'article de la loi fédérale ou provinciale qui régit l'enquête à mener;

D.2.1.5 le nom, le titre et la signature du membre de l'organisme d'enquête qui fait la demande.

D.2.2 Toutes les demandes de renseignements reçues par une institution doivent être conservées.

Documentation des communications en vertu de l'alinéa 8(2)e)

D.2.3 Lorsqu'une telle demande est reçue, le responsable de l'institution ou son délégué responsable des décisions relatives à l'alinéa 8(2)e) de la *Loi* doit conserver un relevé de la communication des renseignements personnels à l'organisme d'enquête. Le relevé doit contenir les renseignements suivants :

D.2.3.1 une indication claire de l'acceptation ou du refus de la demande;

D.2.3.2 la date de réception de la demande;

D.2.3.3 les FRP dans lesquels les renseignements communiqués sont conservés;

D.2.3.4 les renseignements personnels spécifiques, documents ou fichiers qui ont été communiqués;

D.2.3.5 le nom, le titre et la signature de l'agent qui a autorisé la réponse;

D.2.3.6 le nom de l'organisme d'enquête qui a fait la demande.

D.2.4 Un FRP distinct est tenu à jour pour tous les relevés de communication à des organismes d'enquête fédéraux, y compris des copies des renseignements communiqués au demandeur. Comme il est stipulé au paragraphe 8(4) de la *Loi* et à l'article 7 du *Règlement*, les renseignements contenus dans ce FRP doivent être conservés pendant au moins deux ans et communiqués sur demande au Commissaire à la protection de la vie privée.

Annexe E : Norme sur la protection de la vie privée en matière de Web analytique

E.1 Date d'entrée en vigueur

E.1.1 La présente norme entre en vigueur le 26 octobre, 2022.

E.1.2 La présente norme remplace la *Norme sur la protection de la vie privée et le Web analytique* (le 31 janvier 2013).

E.2 Normes

E.2.1 Cette norme contient des détails sur les exigences énoncées à la section 4 de la *Directive sur les pratiques relatives à la protection de la vie privée*.

E.2.2 Les responsables des institutions fédérales ou leurs délégués sont chargés des normes suivantes :

E.2.2.1 Les renseignements recueillis pour le Web analytique qui peuvent être utilisés pour distinguer ou trouver l'identité d'un individu, seuls ou combinés à d'autres renseignements personnels liés ou pouvant être liés à un individu précis, sont considérés des renseignements personnels et sont protégés conformément aux exigences de la *Loi*.

E.2.2.2 Un avis de confidentialité est fourni sur le site Web de l'institution qui comprend les éléments suivants :

E.2.2.2.1 Une explication de ce qu'est le Web analytique et les objectifs de l'utilisation des outils de Web analytique par l'institution;

E.2.2.2.2 Un énoncé indiquant quels renseignements personnels, y compris l'adresse IP, sont automatiquement recueillis sur les visiteurs par l'institution fédérale;

E.2.2.2.3 Une déclaration indiquant quelle est l'autorité légitime pour la collecte de ces renseignements;

E.2.2.2.4 Un énoncé indiquant aux visiteurs si l'adresse IP et d'autres données dans des marqueurs numériques sont recueillies et utilisées à l'interne par l'institution pour le Web analytique ou si elles sont communiquées ou transmises à un fournisseur tiers externe à cette même fin;

E.2.2.2.5 Dans les cas où l'adresse IP et d'autres données dans les marqueurs numériques sont communiquées ou transmises à un tiers, une explication quant à la manière dont la vie privée des visiteurs des sites Web du gouvernement du Canada est assurée grâce, au minimum, à l'activation da la fonction de tout outil du tiers utilisé pour le Web analytique par laquelle le l'adresse IP est dépersonnalisée;

E.2.2.2.6 Si les données communiquées ou transmises pour le Web analytique sont acheminées à l'extérieur du Canada, un énoncé qui l'indique, de même qu'une référence à toutes les lois auxquelles les renseignements pourraient être assujettis; et

E.2.2.2.7 Un énoncé indiquant la période maximale de conservation et la méthode de retrait de tout renseignement personnel recueilli aux fins du Web analytique.

E.2.2.3 Tout contrat mise en place aux fins du Web analytique doit contenir, en plus des exigences précisées à 4.2.24 de la *Directive sur les pratiques relatives à la protection de la vie privée*, les exigences suivantes au minimum :

E.2.2.3.1 Les « renseignements personnels » se définissent comme des renseignements sur un individu recueillis ou générés dans l'exécution du contrat, y compris les types de renseignements décrits spécifiquement dans la *Loi sur la protection des renseignements personnels* et également les renseignements qui peuvent être liés ou sont liés à un individu, comme l'adresse IP du visiteur d'un site Web;

E.2.2.3.2 Le fournisseur tiers doit nommer un agent dans l'organisation qui agira à titre de représentant pour toutes les questions liées aux renseignements personnels en cause et doit fournir le nom et les coordonnées de cet agent à l'institution fédérale dans les 10 jours suivant l'adjudication du contrat;

E.2.2.3.3 Le fournisseur tiers doit informer tous ses employés, contractants et sous-traitants de leurs obligations en matière de protection de la vie privée lorsqu'ils traitent des renseignements personnels communiqués ou transmis dans le

cadre du travail qu'ils accomplissent en vertu du contrat ou de la sous-traitance (le « travail »);

E.2.2.3.4 Le fournisseur tiers doit dépersonnaliser l'adresse IP avant qu'elle ne soit stockée, afin que l'adresse IP complète ne puisse être reconstituée. Cela doit être fait en l'amputant de manière irréversible de son dernier octet ou en employant d'autres techniques qui offrent une protection de la vie privée comparable et qui ont été approuvées par le SCT;

E.2.2.3.5 Le fournisseur tiers ne doit pas lier ou tenter de lier l'adresse IP ou tout identifiant unique apparaissant dans le marqueur numérique lié à l'identité de l'utilisateur d'un ordinateur personnel;

E.2.2.3.6 L'adresse IP rendue dépersonnalisée, ainsi que d'autres données communiquées à un fournisseur tiers pour le Web analytique, doivent être utilisées seulement dans le cadre du travail, et le fournisseur ne doit faire aucune autre utilisation ou réutilisation subséquente de ces données à d'autres fins, à moins d'autorisation écrite préalable de l'institution;

E.2.2.3.7 Le fournisseur tiers ne doit pas communiquer ni transférer l'adresse IP rendue dépersonnalisée ni aucune autre donnée qui lui ont été communiquées sauf pour le travail, avec l'approbation écrite préalable de l'institution ou si la loi l'exige;

E.2.2.3.8 Le fournisseur tiers ne doit utiliser que les témoins internes de premier niveau;

E.2.2.3.9 Le fournisseur tiers n'a pas le droit d'utiliser des techniques qui augmentent le risque d'identification, de réidentification ou de profilage telles que, notamment, l'interconnexion, les renvois croisés, l'exploration de données ou la comparaison de données de sources multiples sur les renseignements personnels recueillis en relation au travail, à moins que ce ne soit autorisé au préalable par l'institution fédérale par écrit;

E.2.2.3.10 Le fournisseur tiers doit mettre en place une protection des renseignements personnels et des renseignements rendus dépersonnalisés qui respecte au minimum la *Politique sur la sécurité du gouvernement*;

E.2.2.3.11 Le fournisseur tiers doit protéger l'adresse IP rendue dépersonnalisée et d'autres données communiquées dans le cadre du travail, et ces données doivent être conservées pendant une période maximale de 6 mois, après quoi les

données, y compris les copies de sauvegarde, doivent être éliminées; et

E.2.2.3.12 Une disposition relative aux vérifications en vertu de laquelle le fournisseur tiers peut faire l'objet d'une vérification, qui comprend une vérification à une date qui sera déterminée par le gouvernement du Canada, au moins une fois dans l'année pour garantir le respect de ces exigences.

E.2.3 Les personnes autorisées à effectuer le Web analytique sur les serveurs de l'institution fédérale ou sur des serveurs hébergés par des fournisseurs tiers sont responsables des normes suivantes :

E.2.3.1 La fonction de tout outil du tiers utilisé pour le Web analytique grâce à laquelle les adresses IP sont dépersonnalisées est activée.

E.2.3.2 Les renseignements personnels ne doivent être utilisés qu'aux fins de Web analytique ou dans un but pour lequel le renseignement peut être communiqué par l'institution aux termes du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

E.2.3.3 Des renseignements personnels recueillis pour le Web analytique ne peuvent pas être utilisés pour ce qui suit :

E.2.3.3.1 à des fins administratives, au sens de la *Loi sur la protection des renseignements personnels*, à moins que la loi ne l'autorise; ou

E.2.3.3.2 aux fins de profilage de personnes identifiables, ce qui comprend la production d'inférences ou d'autres dérivations à partir des renseignements personnels.

E.2.3.4 L'adresse IP et tout autre renseignement personnel y compris, sans s'y limiter, l'information se trouvant dans les marqueurs numériques employés dans le cadre du Web analytique doivent être protégés conformément aux principes énoncés à la section 4.3 de la *Directive sur les services et le numérique*.

E.2.3.5 L'adresse IP et tout autre renseignement personnel y compris, sans s'y limiter, l'information se trouvant dans les marqueurs numériques employés dans le cadre du Web analytique ne peuvent être conservés que pour une période maximale de 18 mois, à l'issue de laquelle ces renseignements doivent être détruits conformément aux exigences 4.2.30 et 4.2.33 de la *Directive sur les pratiques relatives à la protection de la vie privée* et tel qu'autorisé par le bibliothécaire et archiviste du Canada.

ISBN: 978-0-660-71386-1