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

Document d’orientation pour aider à préparer des Ententes d’échange de renseignements personnels

Publié : le 2023-08-22

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

No de catalogue BT39-76/2023F-PDF
ISBN: 978-0-660-67712-5

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: Guidance on Preparing Information Sharing Agreements Involving Personal Information

Document d’orientation pour aider à préparer des Ententes d’échange de renseignements personnels

Sur cette page

Modèle : Entente d’échange de renseignements entre institutions fédérales (DOC (Word Document), 82 KO (Kilo octets))

Modèle : Annexes (DOC (Word Document), 67 KO (Kilo octets))

Introduction et contexte

Le présent document d’orientation est conçu pour aider les parties à remplir le modèle d’entente d’échange de renseignements (EER) et les annexes connexes lors de l’échange de renseignements personnels entre institutions fédérales. Chaque EER est unique et le modèle et le contenu doivent être adaptés à vos besoins.

Le présent document doit être pris en considération parallèlement avec les lois, règlements, politiques et lignes directrices applicables du gouvernement fédéral. Une évaluation détaillée peut être nécessaire pour déterminer les risques d’entrave à la vie privée avant de pouvoir mettre en œuvre une EER. Avant de conclure une EER, les parties sont fortement encouragées à consulter le coordonnateur de l’AIPRP de leur institution, les conseillers en matière de protection des renseignements personnels, les conseillers juridiques, les experts en gestion de l’information et les experts

en sécurité afin de déterminer les lois et politiques qui peuvent avoir une incidence sur les questions de protection des renseignements personnels et de sécurité, et de pouvoir les examiner et les prendre en considération.

Dans le cadre du présent document, à moins d'indication contraire, les EER doivent être considérées comme non juridiquement contraignantes entre deux ou plusieurs institutions fédérales.

Définitions : renseignements personnels et entente d'échange de renseignements

Qu'est-ce qu'un renseignement personnel?

Selon l'article 3 de la *Loi sur la protection des renseignements personnels*, par renseignements personnels, on entend les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable. En voici quelques exemples :

- les coordonnées, les renseignements relatifs à la race, à l'origine nationale ou ethnique, à la couleur, à la religion, à l'âge ou à la situation de famille;
- les renseignements relatifs à l'éducation, au dossier médical, au casier judiciaire ou aux antécédents professionnels de l'individu;
- tout renseignement pouvant être lié à l'identification d'un individu, tel qu'un numéro de compte, un numéro de permis, une adresse IP (protocole Internet), un identifiant biométrique ou une photographie.

Certains renseignements sont exclus de la définition des renseignements personnels. Par exemple, les renseignements qui concernent le poste ou les fonctions d'un employé d'une institution fédérale ne sont pas considérés comme des renseignements personnels.

Le nom d'une personne n'est pas toujours le seul facteur qui détermine si des renseignements sont considérés comme des renseignements personnels. Les renseignements personnels comprennent les renseignements consignés qui peuvent, seuls ou combinés à des renseignements provenant de sources autrement disponibles, y compris des sources publiques, mener à l'identification possible d'un individu. Par « identification possible », on entend une possibilité sérieuse. Il doit s'agir de quelque chose de plus qu'une chance frivole, mais de moins que la « prépondérance des probabilités ».

Dans le cadre du présent document d'orientation, le terme « renseignements personnels » doit être interprété au sens large. Il comprend aussi les « données » lorsqu'elles se rapportent à un individu identifiable.

Qu'est-ce qu'une entente d'échange de renseignements (EER)?

La *Loi sur la protection des renseignements personnels* ne fait aucune référence aux EER. Cela dit, les exigences de base concernant les EER se trouvent aux paragraphes 4.2.23 à 4.2.27 de la Directive sur les pratiques relatives à la protection de la vie privée.

L'« échange de renseignements » peut signifier que l'une des parties communique des renseignements et que l'autre partie en collecte, ou que des renseignements sont échangés, les deux parties communiquant et collectant des renseignements.

Les avantages de l'utilisation d'une EER pour échanger des renseignements personnels entre les institutions fédérales sont les suivants :

- clarifier les obligations et les responsabilités des parties concernées;
- veiller au respect de la *Loi sur la protection des renseignements personnels* et de ses politiques connexes;

- établir des protocoles pour traiter les incidents de sécurité, y compris les atteintes à la vie privée;
- sensibiliser le personnel et lui fournir des instructions;
- assurer la transparence pour les personnes concernées.

Déterminer si une EER est l'outil approprié

Les renseignements à échanger sont-ils des renseignements personnels?

☐ Oui
☐ Non

Avez-vous examiné les renseignements à échanger pour déterminer s'ils comportent des renseignements personnels au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*?

Pour plus de détails à ce sujet, voir la
définition de « renseignements personnels »

S'il ne s'agit pas de renseignements personnels, veuillez consulter les solutions de rechange à l'échange des renseignements personnels avec d'autres institutions ci-dessous.

Avez-vous vérifié votre autorisation légale?

☐ Oui
☐ Non

Si votre institution souhaite recevoir des renseignements personnels, avez-vous vérifié si elle a l'autorisation légale (loi, règlement ou décret) de collecter des renseignements personnels?

Il est recommandé de consulter vos services juridiques afin de vous assurer d'avoir l'autorisation.

Si vous n’avez pas l’autorisation légale de collecter ou d’échanger des renseignements personnels, vous ne devez pas procéder à une quelconque activité d’échange de renseignements personnels.

Avez-vous besoin d’une EER?

- ☐ Oui
- ☐ Non

Il est recommandé d’établir une EER avant d’échanger tout renseignement personnel. Si l’échange des renseignements personnels est exigé par la loi fédérale, l’institution doit le faire conformément aux exigences de cette loi. Dans ce cas, une EER est recommandée, mais pas strictement nécessaire.

Solutions de rechange à l’échange des renseignements personnels avec d’autres institutions

Compte tenu des conséquences possibles de l’échange de renseignements personnels sur la vie privée, les parties doivent examiner si d’autres approches seraient plus appropriées.

Dans la mesure du possible, les renseignements personnels doivent être collectés directement auprès des personnes concernées plutôt que par le biais d’une EER.

Une autre solution consiste à envisager l’utilisation et l’échange de renseignements personnels dépersonnalisés. Les renseignements dépersonnalisés sont des renseignements personnels qui ont été modifiés de telle sorte que le risque d’identifier la personne est fortement diminué et ne peut être facilement réalisé.

Dans de tels cas, la possibilité de relier les renseignements à des individus identifiables ou de faire des déductions indues à propos de groupes d'individus doit rester faible, voire nulle.

Il est recommandé de demander conseil à des experts en statistiques lors de la dépersonnalisation de données. De cette façon, il sera possible de s'assurer que les renseignements à communiquer ne permettent pas d'identifier les individus. Vous pouvez également contacter les experts de la protection des renseignements personnels de votre institution pour vous aider à déterminer le niveau de dépersonnalisation requis compte tenu de l'échange de renseignements que vous proposez. Vous trouverez des conseils supplémentaires sur la dépersonnalisation, en particulier lorsque vous travaillez avec de petites populations, dans l'Avis de mise en œuvre de la protection des renseignements personnels 2023-01 : Dépersonnalisation et dans 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.

Lors de la rédaction de l'EER, assurez-vous :

- d'avoir examiné la possibilité d'échanger des renseignements dépersonnalisés plutôt que des renseignements personnels;
- d'inclure dans l'EER des clauses interdisant à la partie destinataire de repersonnaliser les renseignements personnels et interdisant l'échange ultérieur de ces renseignements dépersonnalisés lorsque des renseignements dépersonnalisés doivent être utilisés.

Si les renseignements personnels ne sont pas requis, vous pouvez envisager d'autres types d'ententes, tels qu'un protocole d'entente, un accord-cadre ou un accord sur les niveaux de service, comme l'indique la Ligne directrice sur les ententes de services — Éléments essentiels.

Échanger les renseignements disponibles au sein de votre institution

Dans certains cas, des lois autres que la *Loi sur la protection des renseignements personnels* permettent explicitement des utilisations ou des communications, au sein de l'institution ou à l'extérieur de celle-ci. Par exemple, la *Loi de l'impôt sur le revenu*, la *Loi sur la statistique*, la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et la *Loi sur le ministère de l'Emploi et du Développement social* contiennent des autorisations spécifiques pour l'utilisation ou la communication de renseignements personnels.

Le secteur de programme qui a le contrôle des renseignements personnels à communiquer peut déterminer si la communication est opportune ou non, d'après les conseils des experts des services juridiques et de la protection des renseignements personnels de l'institution. Il peut y avoir d'autres solutions de rechange, mais les avantages et les risques pour la protection des renseignements personnels associés à une option doivent être évalués avant qu'une décision ne soit prise.

Définition de la portée de l'EER

Toutes les parties à une EER doivent prendre en compte ce qui est directement lié à l'activité pour s'assurer que seule la quantité minimale de renseignements personnels est communiquée et collectée. L'EER doit comprendre une liste de tous les éléments de renseignements personnels qui seront échangés, l'objectif d'échanger chaque élément, ainsi que les restrictions particulières qui peuvent s'appliquer à chacun d'eux (par exemple, il serait bon de préciser que des éléments de renseignements personnels plus sensibles nécessitent des mesures de protection plus

rigoureuses ou d'imposer des conditions plus strictes sur l'utilisation ou la communication ultérieures, par exemple, si le numéro d'assurance sociale est communiqué).

La communication de trop de renseignements personnels ou la collecte de plus de renseignements personnels que nécessaire pour atteindre un objectif particulier sont contraires à la *Loi sur la protection des renseignements personnels* et peuvent entraîner une atteinte à la vie privée.

Évaluation des risques

En plus de s'assurer qu'elles disposent de l'autorisation légale pour effectuer leurs initiatives d'échange de renseignements, les parties doivent s'assurer que tous les risques connexes pour la protection de la vie privée et la sécurité sont pris en compte avant de conclure toute entente d'échange de renseignements personnels.

Les risques pour la vie privée et la sécurité peuvent être évalués de manière cohérente en utilisant les outils recommandés tels que l'évaluation des facteurs relatifs à la vie privée (EFVP), le protocole relatif à la protection des renseignements personnels ou l'évaluation de sécurité et autorisation (ESA), anciennement appelée l'évaluation de la menace et des risques (EMR), lesquels sont décrits ci-dessous.

Évaluation des facteurs relatifs à la vie privée (EFVP)

La Directive sur l'évaluation des facteurs relatifs à la vie privée décrit un processus qui fournit aux décideurs les éléments suivants :

- une évaluation de la conformité de l'initiative avec la *Loi sur la protection des renseignements personnels* et les politiques connexes;

- les répercussions probables liées aux problèmes ou à la non-conformité;
- des stratégies d'atténuation et des échéances pour réduire ou éliminer les risques pour la protection des renseignements personnels.

Protocole relatif à la protection des renseignements personnels

En vertu de la Politique sur la protection de la vie privée, le protocole relatif à la protection des renseignements personnels est un ensemble de procédures consignées et conformes aux principes de la *Loi sur la protection des renseignements personnels* pour l'utilisation des renseignements personnels à des fins non administratives telles que la recherche, les statistiques, l'audit, l'évaluation et l'analyse de politiques.

Évaluation de la sécurité et autorisation (ESA)

Lorsqu'elles échangent des renseignements personnels, les parties doivent mettre en place des mesures de protection administratives, techniques et physiques efficaces pour protéger ces renseignements. Une ESA est un processus par lequel les institutions fédérales s'assurent que des mesures de protection appropriées sont mises en œuvre dans leurs environnements physiques et technologiques. S'il y a lieu, toutes les parties participant à l'initiative d'échange de renseignements pourraient être tenues de suivre ce processus d'évaluation afin d'évaluer les menaces et les risques pour les renseignements comme condition préalable à l'échange ou d'exiger la confirmation que de telles mesures de protection sont mises en œuvre et révisées périodiquement pour assurer la protection des renseignements.

Consignation de la décision

Conformément au paragraphe 4.3.2.10 de la Politique sur les services et le numérique, les administrateurs généraux sont tenus de consigner les décisions et les processus décisionnels. Lors de la conclusion d'une EER, il est recommandé aux parties de résumer les mesures de diligence raisonnable qui ont permis aux dirigeants autorisés des institutions de déterminer qu'une EER était nécessaire. La documentation appropriée peut comprendre une note de service au responsable de programme, une analyse juridique à l'appui, une EFVP ou une ESA.

Rédaction de l'EER et remplissage du modèle d'EER

Une EER devrait établir les modalités qui régiront l'échange de renseignements personnels entre les parties. Un modèle d'EER et les annexes connexes pour les institutions fédérales sont fournis dans le cadre du présent document d'orientation. L'EER doit être spécifique et précise, rédigée dans un langage clair et simple afin que tous les termes soient bien compris, offrir une certaine souplesse pour permettre des modifications limitées, et être rédigée avec l'aide de responsables de programme et de projet, d'experts de la politique sur la protection de renseignements personnels et de la gestion de l'information, de conseillers juridiques et de spécialistes fonctionnels, tels que des spécialistes des systèmes de technologie de l'information et des experts de la sécurité.

Bien que ce guide concerne les échanges de renseignements personnels entre les institutions fédérales, les échanges de renseignements personnels avec les institutions publiques d'autres administrations devraient comprendre des sections semblables à celles du modèle d'EER, mais tenir compte des lois pertinentes des administrations en question.

Un résumé de l'EER doit être rendu public conformément au paragraphe 4.2.26 de la Directive sur les pratiques relatives à la protection de la vie privée. Pour plus de transparence, les institutions peuvent envisager de communiquer l'intégralité de l'EER par l'entremise du Portail du gouvernement ouvert ou sur le site Web de l'institution. Pour plus de renseignements sur l'utilisation du Portail du gouvernement ouvert, veuillez contacter l'équipe de gouvernement ouvert au open-ouvert@tbs-sct.gc.ca.

Éléments d'une de l'EER

▼ Dans cette section

Les sections suivantes fournissent des conseils supplémentaires pour aider les parties dans l'utilisation du modèle d'EER et les annexes fournis. Les institutions qui utilisent leur propre modèle peuvent toujours bénéficier des conseils, mais la terminologie et la structure peuvent ne pas être exactement les mêmes que celles présentées ici.

1. Préambule

Le préambule de l'EER doit exposer les raisons de l'entente, expliquer pourquoi les renseignements sont échangés au lieu d'être collectés directement auprès des personnes concernées, décrire les résultats éventuels que l'institution cherche à atteindre dans le cadre de l'entente et fournir des renseignements généraux pertinents.

Les institutions fédérales qui demandent de recevoir des renseignements personnels doivent pouvoir clairement établir la raison pour laquelle les renseignements sont requis. Les renseignements peuvent être nécessaires à des fins administratives dans les cas où ils seront utilisés dans le cadre d'un processus décisionnel qui touchera les personnes concernées, notamment pour les raisons suivantes :

- **authentification et vérification** : lorsque les renseignements personnels sont utilisés pour comparer et confirmer l'identité des personnes avant d'accorder l'accès à des programmes et des services, à des zones physiques ou à des renseignements;

- **admissibilité à un programme ou à un service** : lorsque les renseignements personnels sont utilisés pour déterminer ou vérifier l'admissibilité à des programmes, administrer des paiements ou des paiements en trop de programmes, ou octroyer ou refuser des permis ou licences;
- **activités de conformité ou de réglementation** : lorsque les renseignements sont utilisés pour déceler d'éventuelles utilisations abusives de programmes ou de services ou du harcèlement et que les conséquences sont de nature administrative (par exemple, amende, interruption des prestations, vérification de demandes ou de dossiers personnels);
- **enquêtes criminelles et application de la loi/sécurité nationale** : lorsque les renseignements sont utilisés à des fins d'enquête et d'application de la loi dans un contexte criminel ou associées à la sécurité nationale ou à des activités antiterroristes.

2. Dispositions

Par souci de clarté et pour faciliter le suivi d'une EER par une institution, il est recommandé que les EER fournissent des détails sur le type d'entente et la durée de l'entente.

Il existe différents types d'EER.

- **Communication unidirectionnelle** : une institution communique des renseignements personnels à une autre institution, sans recevoir elle-même des renseignements.
- **Communication bidirectionnelle** : les deux institutions parties à l'EER reçoivent et communiquent des renseignements personnels.
- **Communication multipartite unidirectionnelle** : une institution communique des renseignements personnels à deux ou plusieurs

autres institutions, sans en recevoir elle-même.
- **Communication multipartite bidirectionnelle** : plus de deux institutions recueillent, utilisent et communiquent des renseignements personnels.

Il existe différentes durées pour les EER.

- **Une seule communication** : les institutions communiquent des renseignements personnels à une seule occasion. Dans ce cas, les renseignements ne peuvent être fournis qu'une seule fois, et l'EER doit indiquer clairement une date d'entrée en vigueur et une date d'expiration.
- **Communication pour une période déterminée** : les renseignements peuvent être communiqués de façon régulière pendant une période déterminée. L'EER doit indiquer clairement une date d'entrée en vigueur et une date d'expiration. Lorsque la période définie dépasse cinq ans, il convient d'ajouter une clause de révision pour garantir que l'EER est révisée sur une base périodique à déterminer par les parties.
- **Communication pour une période indéterminée** : les renseignements personnels peuvent être communiqués de façon régulière pendant une période non spécifiée. L'EER doit inclure une date d'entrée en vigueur et une clause de révision périodique.

3. Autorisation légale pour la collecte et la communication

Collecte

L'article 4 de la *Loi sur la protection des renseignements personnels* interdit aux institutions fédérales de recueillir des renseignements personnels à moins qu'ils n'aient un lien direct avec un programme ou une activité de l'institution fédérale.

La *Loi sur la protection des renseignements personnels* n'est pas la seule source de droit qui fixe les règles qui s'appliquent aux institutions fédérales en matière de collecte, d'utilisation et de communication des renseignements personnels.

D'autres lois fédérales contiennent des dispositions qui autorisent, interdisent ou réglementent expressément l'échange de renseignements personnels. Par exemple, la *Loi sur la statistique* autorise Statistique Canada à conclure des ententes avec des organismes statistiques provinciaux, des institutions fédérales, provinciales ou municipales ou des sociétés.

Quand elles envisagent un échange de renseignements personnels pour la première fois, les parties doivent confirmer que l'échange en question est légal. Par conséquent, toutes les institutions participant à l'échange proposé doivent s'assurer qu'elles disposent de leur propre autorisation légale pour effectuer les activités d'échange de renseignements proposées (collecte et/ou communication).

Avis

Avec une autorisation légale confirmée, les institutions sont tenues d'informer les individus d'une collecte de renseignements personnels. Conformément au paragraphe 5(2) de la *Loi sur la protection des renseignements personnels*, les parties doivent informer les participants au programme, au moment de la collecte, de la nécessité de partager leurs renseignements personnels comme condition d'inscription au programme. Les avis doivent inclure les éléments décrits dans la Directive sur les pratiques relatives à la protection de la vie privée. Par exemple, dans le cadre de nombreux programmes de prestations, il peut être nécessaire que des renseignements personnels soient échangés entre les institutions pour déterminer l'admissibilité aux prestations du programme.

Lors de la rédaction de l'EER, il faut s'assurer :

- que dans la mesure du possible, les personnes sont informées de la nouvelle collecte/communication au point de collecte;
- qu'un avis de confidentialité a été accepté par toutes les parties de l'EER et répond aux exigences de la politique

Remarque : les avis de confidentialité doivent informer la personne de la raison pour laquelle il faut recueillir les renseignements, de toute autorisation légale pour la collecte, de la manière dont les renseignements seront utilisés, avec qui ils seront échangés et dans quel but.

Communication

L'article 8 de la *Loi sur la protection des renseignements personnels* stipule que les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués sans le consentement de l'individu qu'ils concernent, à moins que la communication ne soit autorisée dans l'une des 13 circonstances prévues au paragraphe 8(2). Toutes les dispositions du paragraphe 8(2) relatives à la communication sont de nature discrétionnaire et toute communication de renseignements personnels en vertu de ce paragraphe doit être examinée au cas par cas.

Dans certains cas, les articles de la *Loi sur la protection des renseignements personnels* qui autorisent la communication ne précisent pas qui doit prendre la décision. Bien qu'aucune règle ne précise qui devrait être cette personne, il est important qu'un représentant approprié soit désigné comme ayant pris la décision de communiquer les renseignements, par souci responsabilisation et de transparence.

L'échange de renseignements personnels pourrait, dans certaines situations, mettre en cause la *Charte canadienne des droits et libertés* (la Charte). Le fait qu'une communication soit spécifiquement autorisée par

d’autres lois fédérales ne garantit pas automatiquement la conformité avec la Charte. Ce n’est pas un secret que les liens entre ces domaines de droit sont assez complexes et que des conseils juridiques seront nécessaires.

Lors de la rédaction de la section 3 de l’EER, assurez-vous que :

- votre EER ne prévoit que la collecte de renseignements personnels qui sont « directement liés à un programme ou à une activité de votre institution »;
- vous avez consulté vos services juridiques pour établir l’autorisation de collecte :
    - le consentement (décrit ci-dessous) n’est pas une autorisation suffisante pour collecter des renseignements personnels;
- vous avez consulté l’ensemble des instruments de politique sur la protection des renseignements personnels du SCT, y compris la Directive sur le numéro d’assurance sociale, si vous avez l’intention de recueillir ou de communiquer le NAS;
- vous avez déterminé si l’entente prévoit une communication visée par une disposition du paragraphe 8(2);
- vous avez vérifié si la loi habilitante de votre institution est plus restrictive que le paragraphe 8(2) de la *Loi sur la protection des renseignements personnels* en ce qui concerne la communication de renseignements personnels

4. Exactitude des renseignements personnels et respect des normes

Exactitude

Les parties à une EER doivent fonder leurs décisions administratives sur des renseignements personnels actuels et à jour. Cela est particulièrement important lorsque l’incidence d’une décision administrative sur les

individus peut être élevée. Fournir des renseignements non fiables, inexacts ou incomplets à d'autres institutions peut créer des problèmes potentiellement graves pour ceux qui se fient à ces renseignements ainsi que pour ceux qui font l'objet de ces inexactitudes.

Lors de la rédaction, assurez-vous que l'EER :

- contient une obligation d'informer l'autre partie si l'institution a connaissance de renseignements personnels inexacts qui ont été échangés;
- contient une disposition selon laquelle l'autre partie doit revoir toute mesure administrative prise sur la base de renseignements inexacts fournis;
- comprend un processus pour traiter toute demande de correction présentée par l'individu concerné.

Normes applicables

Les institutions doivent faire tous les efforts raisonnables pour garantir que tous les renseignements personnels communiqués, notamment les métadonnées associées utilisées pour les décrire, sont pertinents et répondent aux normes applicables (par exemple, qualité). Cela est particulièrement important lorsque les renseignements personnels seront utilisés dans un processus décisionnel qui touche les individus. Avant d'échanger les renseignements, les parties doivent clairement établir le type, l'étendue et la qualité des renseignements personnels et des métadonnées associées à échanger, ainsi que la méthode de transmission. Les parties devront peut-être prendre les mesures nécessaires pour s'assurer que les renseignements personnels conviennent à l'utilisation prévue avant de conclure une entente pour les échanger.

Les renseignements criminels sont un exemple de l'importance de s'assurer que les renseignements personnels qui en contiennent sont conformes aux normes. Dans de tels cas, l'institution fédérale qui communique les renseignements peut indiquer la fiabilité des renseignements en question en fournissant des renseignements généraux, notamment s'ils ont été observés, entendus d'une source ou obtenus par interception électronique, et leur origine. Dans cet exemple, l'EER devrait comprendre des mises en garde pour répondre à toute préoccupation concernant la qualité des renseignements personnels ou des métadonnées qui les décrivent.

La section 4.3 du modèle d'EER comprend des dispositions relatives aux normes que l'institution doit respecter pour s'assurer que les renseignements personnels sont de grande qualité.

Lors de la rédaction de l'EER, assurez-vous que :

- le format des renseignements personnels, y compris les métadonnées associées, est précisé dans l'EER de manière à ce qu'ils soient « lisibles » par l'autre partie, les renseignements et métadonnées échangés devant être interopérables entre les parties et normalisés conformément à la Politique sur les services et le numérique et à la Norme sur les métadonnées;
- le profil et la validation des renseignements personnels reçus de parties externes, gouvernementales ou autres, ont été effectués avant de les utiliser ou de les réutiliser, une pratique qui nécessite de respecter toutes les normes pertinentes au niveau de l'organisation pour en assurer l'interopérabilité structurelle et sémantique;
- s'il y a lieu, les échanges de renseignements seront enregistrés ou consignés de manière adéquate dans le dossier de l'individu concerné

par l’institution qui communique les renseignements, au cas où il serait nécessaire de corriger des renseignements inexacts.

5. Utilisation

L’article 7 de la *Loi sur la protection des renseignements personnels* interdit à une institution fédérale d’utiliser des renseignements personnels sans le consentement de l’individu qu’ils concernent, sauf pour les fins auxquelles ils ont été collectés ou pour un usage compatible avec ces fins.

Utilisation secondaire

Toute interdiction d’utilisation secondaire doit être acceptée avant de conclure une entente d’échange de renseignements personnels. Le cas échéant, les procédures permettant de demander l’autorisation d’une utilisation supplémentaire doivent être définies dans l’EER, en tenant compte des lois, règlements ou politiques applicables à chaque partie à l’EER.

Lors de la rédaction, assurez-vous que l’EER :

- indique comment seront utilisés les renseignements personnels qui seront échangés en vertu de l’EER;
- décrit toute utilisation secondaire prévue et est mise à jour lorsque de nouvelles utilisations secondaires sont déterminées;
- précise que les utilisations secondaires sont limitées à celles qui sont conformes à l’article 7 de la *Loi sur la protection des renseignements personnels*;
- décrit toute restriction concernant l’utilisation ultérieure ou secondaire des renseignements, en tenant compte des lois, règlements ou politiques qui s’appliquent à chaque partie à l’EER;
- contient des clauses définissant les procédures à suivre pour obtenir l’approbation d’une utilisation ultérieure, ainsi que toute autre

condition appropriée.

6. Communication

Le paragraphe 8(2) de la *Loi sur la protection des renseignements personnels* décrit les circonstances dans lesquelles les renseignements personnels qui relèvent d'une institution fédérale peuvent être communiqués sans le consentement de l'individu auquel ils se rapportent. De telles communications sont discrétionnaires et sont soumises à toute autre loi du Parlement.

Il convient de noter que l'alinéa 8(2)*j*) de la *Loi sur la protection des renseignements personnels* autorise le responsable d'une institution fédérale à communiquer des renseignements personnels à toute personne ou tout organisme à des fins de recherche ou de statistique, si le responsable de l'institution fédérale qui a le contrôle des documents :

- est convaincu que les fins auxquelles les renseignements sont communiqués ne peuvent raisonnablement être atteintes que si les renseignements sont fournis sous une forme qui permettrait d'identifier l'individu qu'ils concernent;
- obtient de la personne ou de l'organisme un engagement écrit selon lequel les renseignements ne seront pas ultérieurement communiqués sous une forme qui risquerait vraisemblablement de permettre d'identifier l'individu qu'ils concernent.

Communication secondaire

Toute interdiction de communications secondaires doit être acceptée avant de conclure une entente d'échange de renseignements personnels. Le cas échéant, les procédures permettant de demander l'autorisation d'une

communication supplémentaire doivent être définies dans l'EER, en tenant compte des lois, règlements ou politiques applicables à chaque partie à l'EER.

Lors de la rédaction, assurez-vous que l'EER :

- indique comment seront communiqués les renseignements personnels qui seront échangés en vertu de l'EER;
- décrit toutes les communications secondaires prévues et est mise à jour lorsque de nouvelles communications secondaires sont déterminées.

Lorsqu'il s'agit de déterminer si une communication potentielle est conforme au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*, les institutions devraient faire appel à des experts de la protection des renseignements personnels et du domaine juridique.

7. Droits d'accès

Les EER peuvent faire l'objet d'une demande d'accès à l'information et de renseignements personnels. À ce titre, l'EER doit comprendre des clauses concernant le processus qui sera utilisé pour répondre à une telle demande et indiquer si les parties veulent être consultées, comment le processus de consultation doit être mené et quelle partie doit être responsable du traitement de la demande.

Lors de la rédaction de l'EER, assurez-vous qu'elle :

- contient des clauses visant à établir une procédure de consultation pour répondre aux demandes présentées en vertu de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels*;
- comprend des clauses obligeant les parties à s'informer mutuellement lorsqu'elles reçoivent une demande d'accès à l'information et qu'elles

ont l’intention de communiquer des renseignements.

8. Méthode de communication et fréquence de la communication

Définir la méthode de communication des renseignements et la fréquence de la communication est important pour garantir que la collecte et la communication des renseignements personnels se déroulent comme prévu par les deux parties et qu’elles sont conformes aux exigences des lois et des politiques. En outre, en déterminant la méthode et la fréquence des communications, les institutions seront mieux préparées à réagir rapidement en cas d’accès non autorisé aux renseignements ou de traitement inapproprié de ceux-ci.

Les renseignements peuvent être soit « transmis » (à l’initiative de la partie qui les communique), soit « demandés » (à l’initiative de la partie qui les reçoit). Quelle que soit la méthode utilisée, les institutions ne doivent transférer que les renseignements pertinents à l’autre partie et seulement de la manière, aux heures et aux dates prévues par l’EER, plutôt que de donner un accès continu à la base de données dans laquelle les renseignements personnels sont stockés.

Lors de la rédaction, assurez-vous que l’EER :

- établit le processus et la fréquence, qui ont été acceptés par les parties, selon lesquels les renseignements personnels seront communiqués d’une partie à l’autre. Voir l’annexe D — Transmission et protection des renseignements pour des exemples de rédaction possible;
- comprend des processus et des technologies de rechange pour l’échange au cas où le processus ou la technologie principale serait temporairement indisponible.

9. Gestion de l’information

Les renseignements collectés, utilisés, communiqués ou éliminés doivent être gérés conformément à la législation, à la Politique sur les services et le numérique, à la Politique sur la protection de la vie privée et aux instruments de politique à l’appui. Voir l’annexe D — Transmission et protection des renseignements pour obtenir d’autres informations.

La Directive sur les services et le numérique exige que les institutions utilisent les systèmes numériques comme moyen privilégié de gestion de l’information. L’exploitation des systèmes intégrés dans la mesure du possible peut accroître l’efficacité de l’échange de renseignements.

Les institutions fédérales doivent faire en sorte que leurs pratiques et contrôles de gestion de l’information soient définis, documentés, mis en œuvre, évalués, surveillés et tenus à jour tout au long des étapes du cycle de vie de l’information afin de fournir une assurance raisonnable que l’information est protégée de manière adéquate, dans le respect des obligations légales et autres, et en établissant un juste équilibre entre le risque de préjudice et les menaces et le coût de l’application des mesures de protection.

Les parties doivent prendre des mesures pour s’assurer que leurs pratiques de gestion de l’information sont conformes à celles avec lesquelles les renseignements personnels sont ou seront échangés. Le Cadre de l’architecture intégrée du gouvernement du Canada définit les exigences en matière d’architecture intégrée qui permettent de garantir l’harmonisation des pratiques de gestion de l’information dans l’ensemble du gouvernement.

Lors de la rédaction de l’EER, tenez compte des pratiques exemplaires ci-dessous :

- utiliser des systèmes numériques pour créer, collecter, gérer, utiliser et échanger des renseignements personnels;
- définir clairement les rôles, les responsabilités et les obligations en matière de renseignements personnels au sein de l'institution fédérale par le biais d'une structure de gouvernance ministérielle, tant au niveau opérationnel qu'au niveau des cadres supérieurs;
- veiller, le cas échéant, à ce que les jeux de données relatifs aux renseignements personnels soient mis à jour à intervalles appropriés;
- évaluer régulièrement la valeur et l'utilité des ressources de renseignements personnels afin de s'assurer que la collecte et l'utilisation des renseignements personnels sont limitées à ce qui est nécessaire pour un programme ou une activité.

10. Gestion de la sécurité

Des contrôles de sécurité appropriés sont essentiels pour soutenir la prestation de programmes et de services fiables. Dans le contexte de l'échange des renseignements personnels, il est essentiel que des mesures soient mises en place pour permettre le transfert et le stockage sécurisés des renseignements personnels.

Conformément à la Politique sur la sécurité du gouvernement et au paragraphe 4.5.1 de la Directive sur la gestion de la sécurité, les employés du gouvernement fédéral sont tenus de respecter la Politique de sécurité du gouvernement et les pratiques de sécurité ministérielles, ce qui comprend la protection de l'information et des biens sous leur contrôle, qu'ils travaillent sur place ou hors site.

L'EER doit comprendre des clauses expliquant que les renseignements échangés entre les parties sont traités conformément à la désignation de sécurité des renseignements et sur la base du « besoin de savoir », de sorte

que seuls les employés autorisés aient accès aux renseignements pertinents au moment opportun.

Toute mesure de sécurité appropriée pour garantir la sécurité des renseignements personnels pendant et après leur transmission, telle que le chiffrement, la protection par mot de passe ou l'authentification, doit être indiquée dans l'EER. Le fait d'étiqueter les renseignements échangés ou d'y incorporer des filigranes, surtout quand il s'agit de renseignements sensibles, constitue une façon de s'assurer que les renseignements sont traités conformément aux modalités de l'EER.

La nature des mesures de protection des renseignements personnels contre des risques internes et externes varie selon le caractère sensible des renseignements ayant été recueillis, la quantité, la distribution et la forme ou le support des renseignements, la méthode de stockage et le préjudice susceptible d'être causé par un incident de sécurité. Les renseignements plus sensibles seront protégés par un niveau de sécurité plus élevé. À cette fin, les institutions fédérales, au sens de l'article 11.1 de la *Loi sur la gestion des finances publiques* (LGFP), doivent respecter les exigences de la Politique sur la sécurité du gouvernement, de la Politique sur les services et le numérique, ainsi que d'autres normes et directives connexes. Les institutions qui ne sont pas soumises à la LGFP doivent se reporter à leurs propres politiques et procédures en matière de sécurité.

De plus, les mesures de protection doivent tenir compte des mesures à prendre en réaction à des incidents de sécurité ou à des atteintes à la vie privée, notamment aviser les parties touchées. Pour plus de renseignements, se reporter à l'Annexe B de la Directive sur les pratiques relatives à la protection de la vie privée.

Ces mesures sont souvent comprises dans un calendrier distinct joint à l'EER afin de permettre la modification de celle-ci quand les mesures sont modifiées. L'annexe D — Transmission et protection des renseignements, et l'annexe E — Attestation de prise en compte des exigences de sécurité, fournissent un exemple de texte.

Lors de la rédaction de l'EER, tenez compte des éléments suivants :

- si les renseignements personnels doivent porter un titre ou un filigrane « Reçu à titre confidentiel en vertu de (titre de l'EER) », ce qui pourrait aussi permettre d'identifier la source de renseignements dont la communication n'a pas été autorisée;
- comment les institutions qui concluent une EER s'assurent que les renseignements personnels échangés reçoivent la même classification de sécurité de part et d'autre (voir l'annexe J de la Directive sur la gestion de la sécurité pour plus de détails, et l'annexe F de cette directive, qui contient une série d'exigences de sécurité pour les institutions qui concluent des ententes, qui devraient être respectées par les institutions fédérales de la fonction publique centrale);
- si l'EER vise l'échange de renseignements personnels avec des institutions qui ne sont pas assujetties à la Directive sur la gestion de la sécurité, comme les sociétés d'État, et si des détails supplémentaires doivent être ajoutés aux EER afin que les obligations soient bien comprises par toutes les parties.

11. Gestion des incidents de sécurité et des atteintes à la vie privée présumés

Il faut signaler et gérer efficacement les incidents de sécurité et les atteintes à la vie privée afin de garantir que chaque partie à l'EER respecte les exigences en matière de protection des renseignements personnels et de sécurité. Le modèle d'EER et l'annexe G — Protocole relatif aux incidents

de sécurité présumés, notamment les atteintes à la vie privée exigent la notification de toutes les parties à l'EER de toute atteinte présumée à la vie privée. L'outil de rapport préliminaire peut être utilisé à cette fin.

De nombreuses atteintes à la vie privée sont des incidents de sécurité, il est donc essentiel que les responsables de la protection des renseignements personnels de chaque institution coordonnent leur réponse avec les responsables de la sécurité. De même, tous les incidents de sécurité liés à des ressources d'information doivent être portés à l'attention des responsables de la protection des renseignements personnels, qui sont les mieux placés pour déterminer si les renseignements sont de nature personnelle.

Les exigences supplémentaires en matière de politique comprennent l'établissement de procédures pour aviser les personnes touchées par les atteintes à la vie privée. Le fait d'indiquer dans l'EER quelle institution avisera les personnes dans quelles circonstances pourrait contribuer à rationaliser le processus de gestion des atteintes.

Vous trouverez plus de détails sur la gestion des incidents de sécurité dans la Directive sur la gestion de la sécurité et son Annexe G : Procédures obligatoires relatives aux mesures de sécurité dans la gestion des événements, et des conseils supplémentaires sur la gestion des atteintes à la vie privée peuvent être trouvés dans l'Annexe B de la Directive sur les pratiques relatives à la protection de la vie privée.

Lors de la rédaction de l'EER, assurez-vous que :

- l'EER comprend des exigences en matière d'atteinte à la vie privée en cas de communication, d'utilisation, de modification et de suppression accidentelles ou non autorisés de renseignements personnels, ou d'accès accidentel ou non autorisé à de tels renseignements (voir

l'annexe G du modèle d'EER — Protocole relatif aux incidents de sécurité présumés, notamment les atteintes à la vie privée);

- l'EER exige que chaque partie suive les plans de son institution en cas d'atteinte et contient une recommandation à l'intention des institutions visant l'utilisation du Formulaire de déclaration des atteintes en vertu de la *Loi sur la protection des renseignements personnels* du Commissariat à la protection de la vie privée (CPVP) pour signaler au SCT et au CPVP toute atteinte importante à la vie privée;
- les coordonnées des responsables de la protection des renseignements personnels et de la sécurité font partie des coordonnées fournies dans l'EER;
- l'EER comprend une clause sur la coordination entre les responsables de la protection des renseignements personnels et de la sécurité des institutions.

12. Période de conservation et élimination

Conservation des renseignements personnels

La *Loi sur la Bibliothèque et les Archives du Canada* donne une orientation générale en ce qui concerne la conservation des documents gouvernementaux. De plus, la *Loi sur la protection des renseignements personnels* et le règlement connexe exigent que les renseignements personnels utilisés par une institution fédérale à des fins administratives soient conservés par cette institution pendant au moins deux ans après la dernière utilisation administrative des renseignements, à moins que la personne concernée ne consente à les éliminer plus tôt.

Selon la Directive sur les services et le numérique, chaque institution fédérale est responsable de l'établissement, la mise en œuvre et la tenue à jour des périodes de conservation des ressources documentaires ayant une

valeur opérationnelle. Il incombe à chaque institution fédérale de comprendre et d'appliquer toute loi relative à la conservation et à la communication de l'information et plus particulièrement sa loi habilitante lorsqu'elle fixe ces périodes de conservation.

Les parties à une EER doivent indiquer une période de conservation pour les renseignements personnels échangés dans le cadre de l'EER. Les parties doivent s'assurer que la période de conservation correspond au moins aux deux ans prévus par l'article 7 du Règlement sur la protection des renseignements personnels.

Retrait ou élimination des renseignements personnels

Le retrait ou l'élimination des renseignements personnels est également régie par la *Loi sur la protection des renseignements personnels* et la *Loi sur la Bibliothèque et les Archives du Canada*. Cependant, les exigences en matière de retrait ou d'élimination sont moins prescriptives et sont prévues dans les instruments de politique. Pour cette raison, il est recommandé de consulter les experts en gestion de l'information de votre institution.

Les renseignements échangés dans le cadre d'une EER qui font l'objet d'une mise en suspens en vue d'un litige ne doivent **pas** être éliminés ou retirés avant la fin du litige ou la fin de toutes les possibilités d'appel. Les institutions devraient consulter leurs services juridiques si elles se trouvent dans une telle situation.

L'EER doit expliquer comment les parties prévoient éliminer les renseignements personnels.

Selon le degré de sensibilité des renseignements personnels échangés, les institutions peuvent exiger d'être avisées une fois que les renseignements ont été détruits. Il faudra alors créer un document faisant état de la

destruction ou un registre de retrait ou d'élimination des renseignements personnels échangés.

Ce document ou ce registre peut être immédiatement mis à la disposition de l'autre partie, si elle en fait la demande, et renfermer les renseignements suivants :

- les détails concernant les documents éliminés (par exemple, nom, numéro et date du document);
- la méthode de destruction (copie papier déchiquetée ou version électronique supprimée de tous les dossiers);
- la date de destruction (jour, mois, année);
- le nom et le titre de poste de la personne qui les a détruits.

Les parties à une EER peuvent également utiliser l'annexe F de l'EER — Certificat de destruction de renseignements personnels et d'éléments de données pour attester que les renseignements personnels et les données en leur possession ont été détruits et éliminés.

Lors de la rédaction, assurez-vous que l'EER comprend :

- une période de conservation des renseignements personnels et, si nécessaire, des clauses permettant d'obtenir le consentement des individus pour une destruction anticipée;
- une disposition précisant si les renseignements personnels doivent être retournés à l'institution ou s'ils doivent être détruits par l'institution destinataire au terme de l'EER;
- une disposition précisant si un document de destruction sera utilisé par les institutions parties à l'EER;
- un processus permettant d'avoir connaissance de toute obligation de préservation en cas de litige, toute demande de renseignements personnels ou toute demande d'accès à l'information qui empêcherait

la destruction de tout renseignement personnel pour toutes les parties de l'EER, et de les communiquer.

13. Surveillance de la conformité et audits

Les audits permettent de veiller à ce que les parties à une EER respectent les modalités de l'entente. Les dispositions relatives aux audits contribuent également à renforcer les contrôles de sécurité et de protection des renseignements personnels en incitant les parties à s'assurer que leurs contrôles en matière d'information et de protection des renseignements personnels sont aussi efficaces que possible pour répondre à toutes leurs exigences de conformité.

Lors de la rédaction de l'EER, déterminez :

- si les parties veulent utiliser des audits de gestion pour évaluer leurs pratiques respectives de gestion de l'information et leur conformité aux exigences de l'EER;
- si les parties conviennent de se fournir une copie de leurs rapports de vérification de gestion respectifs et de tout plan d'action dans un délai prescrit après qu'ils sont achevés;
- si les clauses de l'EER doivent prévoir des audits particuliers selon un calendrier prédéterminé.

14. Transparence

Le paragraphe 4.2.27 de la Directive sur les pratiques relatives à la protection de la vie privée exige que les parties s'assurent de respecter les exigences en matière de sécurité lorsqu'elles concluent une EER et en publient un résumé qui contient les renseignements suivants, selon l'Annexe K — Résumé de l'entente à publier :

- le titre de l'EER;

- le nom du programme;
- les institutions fédérales qui sont parties à l'EER;
- la date d'entrée en vigueur;
- la date de fin et/ou de révision (selon le type/la durée de l'EER);
- l'objectif (y compris la raison, le type et la durée de l'EER);
- les autorisations légales;
- les renseignements personnels communiqués et collectés (y compris le titre et le numéro du fichier de renseignements personnels [FRP]).

La *Loi sur la protection des renseignements personnels* exige également que les renseignements personnels qui relèvent de l'institution soient décrits dans un FRP. Lors de la collecte de renseignements personnels par le biais d'une EER, les institutions doivent consulter leurs experts en protection des renseignements personnels pour déterminer le FRP pertinent et vérifier s'il nécessite des changements ou des mises à jour résultant de l'EER.

Lors de la rédaction de l'EER, déterminez les éléments ci-dessous.

- Les exigences en matière de sécurité et les autres considérations juridiques ou de confidentialité qui s'appliquent à la publication de l'EER ou d'un résumé de l'EER. Dans la plupart des cas, un résumé de l'EER devrait être possible, même si certains détails doivent être caviardés.
- La plateforme privilégiée par les parties pour la communication publique : en plus de respecter les exigences de la Directive sur les pratiques relatives à la protection de la vie privée visant la publication de mises à jour annuelles dans Info Source, les parties devraient également envisager d'utiliser les plateformes existantes telles que le Portail du gouvernement ouvert du gouvernement du Canada pour les communications publiques. Lorsque les institutions envisagent d'utiliser le Portail du gouvernement ouvert, elles devraient contacter

l'équipe du gouvernement ouvert au open-ouvert@tbs.sct.gc.ca et se conformer aux politiques et directives du Secrétariat du Conseil du Trésor du Canada (SCT) en matière de gestion de l'information et de communication, telles que la Politique sur les services et le numérique et la Directive sur le gouvernement ouvert.
- S'il y a lieu de consulter les experts en matière de protection des renseignements personnels pour déterminer s'il faut mettre à jour un FRP.

15. Avis

Les parties à une EER doivent s'informer mutuellement, dès que possible, de tout changement dans la législation, la réglementation, les politiques, les technologies ou le financement concernant leurs programmes respectifs qui pourrait avoir une incidence sur leur capacité à remplir leurs obligations telles qu'elles sont décrites dans l'entente.

Tous les avis doivent être faits par écrit par les fonctionnaires désignés qui ont signé l'EER ou leur délégué, conformément à l'annexe H du modèle d'EER. Ils doivent être clairs et concis et avoir pour but de communiquer les changements particuliers qui ont une incidence sur l'EER et peut-être même sur la capacité à respecter les obligations.

Lors de la rédaction des avis, les institutions devraient envisager d'inclure les renseignements suivants :

- les clauses de l'EER sur lesquelles le changement aura une incidence;
- une description claire des événements qui ont conduit au changement;
- si le changement est susceptible d'entraîner un retard;
- le moment où le changement devrait entrer en vigueur;
- les mesures d'atténuation qui ont été ou devront être prises;

- dans les cas où les institutions utilisent le recouvrement des coûts, si le changement aura une incidence sur le montant du recouvrement des coûts.

16. Arrangements financiers

Certaines institutions peuvent vouloir inclure des dispositions de recouvrement des coûts dans les EER qu'elles concluent avec d'autres institutions. La section 16 du modèle d'EER et l'annexe J fournissent des exemples de ce type de dispositions.

Les parties doivent se renseigner au sujet des exigences de la politique financière et confirmer qu'elles disposent des autorisations appropriées pour amorcer le recouvrement des coûts. Les parties devraient se reporter à la Directive sur l'imputation et les autorisations financières spéciales et à la LGFP pour connaître leurs pouvoirs en matière de recouvrement des coûts, en consultation avec les services juridiques de leur institution.

Il convient aussi de déterminer s'il s'agit d'une entente pluriannuelle dans le cadre de laquelle les coûts s'accumulent pendant toute la durée de l'entente, ou d'une entente qui porte sur un exercice particulier dans le cadre de laquelle les revenus ne peuvent être dépensés que pendant l'exercice au cours duquel les coûts ont été engagés.

Les parties à l'EER devront convenir d'un processus et d'un calendrier pour le recouvrement des coûts.

Exemple 1 : L'[institution responsable de la communication des renseignements] enverra des factures trois fois par an. La première facture sera envoyée en août pour couvrir les renseignements fournis en avril et juillet, et la seconde sera envoyée à la mi-février (pour garantir un paiement avant le 31 mars) pour couvrir les renseignements fournis en

octobre et janvier. Si nécessaire, l'[institution responsable de la communication des renseignements] rapprochera les coûts avec les dépenses réelles à ce jour et procédera à un ajustement de l'écart.

Exemple 2 : L'[institution responsable de la communication des renseignements] enverra une facture en septembre de chaque année, après la fourniture annuelle de renseignements, prévue pour le 15 août de chaque année. L'[institution destinataire] accepte de rembourser ces frais à l'[institution responsable de la communication des renseignements]. Si nécessaire, l'[institution responsable de la communication des renseignements] rapprochera les coûts avec les dépenses réelles à ce jour et procédera à un ajustement de l'écart.

17. Examen

Dans les cas où la durée d'une EER dépasse une période de cinq ans, les parties à une EER doivent inclure une clause garantissant que l'EER fait l'objet d'un examen sur une base périodique à déterminer entre les parties. Voir la section 17 — Examen du modèle d'EER pour un exemple d'une telle clause. Des examens plus fréquents peuvent être envisagés si nécessaire.

18. Modifications

Les modifications des modalités d'une EER ou des annexes connexes doivent être communiquées par écrit et signées par les fonctionnaires désignés ou leurs représentants autorisés. Voir la section 18 du modèle d'EER pour un exemple de formulation. Les parties à l'EER doivent inclure dans l'EER des clauses définissant le processus de modification de l'EER ou des annexes connexes.

Dans les cas où une modification vise la collecte, l'utilisation, la communication à des tiers, le transfert entre parties, l'élimination, ou d'autres aspects de la gestion des renseignements personnels, les institutions doivent modifier leurs FRP connexes. Si les modifications sont importantes, les institutions doivent également fournir au SCT le FRP mis à jour ainsi qu'une évaluation des facteurs relatifs à la vie privée, comme le prévoit le paragraphe 4.1.7 de la Directive sur les pratiques relatives à la protection de la vie privée.

Si les modifications apportées aux modalités d'une entente entraînent de nouveaux usages compatibles ou de nouvelles communications, les institutions doivent modifier leurs FRP en conséquence et informer le CPVP de nouveaux usages compatibles, comme le prévoit le paragraphe 4.1.17 de la Directive sur les pratiques relatives à la protection de la vie privée.

Entrée en vigueur

Une EER entre en vigueur à la date d'entrée en vigueur convenue par les parties et reste en vigueur à moins qu'elle ne soit résiliée conformément à la procédure énoncée à la section 19 du modèle ou qu'elle ne soit remplacée par une autre entente.

19. Résiliation

La résiliation d'une EER ou d'une annexe doit se faire par écrit, soit à la suite d'un consentement mutuel des deux parties, soit par la transmission par l'une des parties d'un avis de résiliation à l'autre partie. Un avis doit être fourni au fonctionnaire désigné de l'institution pour l'entente. Malgré la résiliation de l'EER, les conditions qui s'appliquent à l'échange des renseignements personnels et les clauses connexes continuent normalement à s'appliquer aux renseignements qui ont déjà été échangés. Les parties à l'EER doivent inclure des clauses définissant comment les

renseignements doivent être éliminés au terme de l'EER. Lorsque des dispositions relatives au recouvrement des coûts sont incluses dans une EER, l'obligation de rapprochement des comptes et d'envoi d'une facture finale, le cas échéant et sous réserve de la résiliation de l'entente, continue également de s'appliquer.

À la résiliation d'une EER, les parties devraient en informer leur bureau de l'AIPRP et mettre à jour leurs FRP connexes.

Lors de la rédaction de l'EER, assurez-vous que :

- l'EER comporte une clause garantissant qu'elle est révisée sur une base périodique prédéterminée (l'examen des EER au moins tous les cinq ans à partir de leur date de signature ou plus fréquemment est fortement encouragé);
- l'EER comporte des dispositions permettant aux parties de résilier immédiatement l'EER et de demander la restitution des renseignements personnels qui ont été échangés;
- l'EER contient des clauses où les modifications de l'EER et des annexes sont communiquées par écrit et exécutées par les signataires de chaque institution ou leur représentant sous la forme d'une lettre officielle;
- l'EER contient des clauses relatives au processus de modification et des clauses de résiliation.

20. Règlement des différends

En cas de questions, de contestations ou de désaccords concernant tout aspect d'une EER, il est recommandé que des clauses soient incluses afin de prévoir un mécanisme de règlement des différends. La section 21 du modèle d'EER fournit un exemple de texte.

Dans les cas où les différends ne peuvent être résolus, le responsable de l'institution ou le sous-ministre (le cas échéant) constituent généralement le niveau ultime de règlement des différends.

Lors de la rédaction de l'EER, déterminez :

- si l'EER doit contenir des clauses de règlement des différends en cas de questions ou de contestations liées à l'interprétation, ou de désaccords associés à l'EER.

21. Fonctionnaires désignés

Une EER doit comprendre la date, les noms, les titres et les signatures des fonctionnaires désignés de toutes les parties à l'entente. Se reporter à la section 21 du modèle d'EER et aux sections pertinentes des annexes A, B et H pour des exemples.

Le niveau de délégation pour signer des EER dépend du degré de sensibilité des renseignements, de l'ampleur de tout recouvrement de coûts et des pouvoirs conférés par la législation. Les ententes jugées à faible risque ou à faible coût sont souvent signées au niveau du directeur ou du directeur général.

Lorsque les renseignements personnels sont plus sensibles ou que les coûts sont plus élevés, le responsable de l'institution ou un sous-ministre ou un sous-ministre adjoint de niveau équivalent peut signer.

Les EER de plus grande ampleur, qui sont des ententes générales composées d'ententes annexées plus petites, sont souvent signées par les responsables des institutions ou les sous-ministres (le cas échéant). La signature des modifications apportées aux annexes des EER générales

pourrait être déléguée à un représentant autorisé qui serait responsable du domaine du programme. Cette façon de faire permet une plus grande flexibilité si le contenu de ces annexes doit être modifié.

En général, le signataire des parties aux EER est de niveau équivalent, mais cela peut différer si un signataire particulier est indiqué dans la législation. Par exemple, si le sous-ministre signe l'EER pour la partie A, le sous-ministre ou une personne de niveau équivalent devrait être le signataire pour la partie B. Cette pratique s'étend aux EER intergouvernementales, où le signataire provincial ou territorial serait au même niveau que son homologue fédéral.

Définitions

Les définitions des termes « fins administratives », « responsable de l'institution fédérale », « renseignements personnels » et « fichier de renseignements personnels » qui figurent ci-après sont conformes aux définitions de ces expressions qui figurent à l'article 3 de la *Loi sur la protection des renseignements personnels*. Les autres définitions ont été adaptées aux fins du présent document d'orientation.

avis (notice)
Notification transmise à une autre institution concernant d'éventuelles modifications d'une EER.

Avis de confidentialité (privacy notice)
Avis verbal ou écrit informant une personne des fins pour lesquelles les renseignements personnels sont recueillis et de l'autorisation de collecte accordée à l'institution fédérale, notamment de créer, d'utiliser et de communiquer les renseignements. L'énoncé, qui doit faire référence au FRP décrit dans Info Source, informe également la personne de son droit d'accéder aux renseignements personnels et d'en demander la correction,

ainsi que des conséquences du refus de fournir les renseignements demandés.

consentement (consent)
Accord éclairé et volontaire d'une personne relativement à la collecte indirecte ou à la communication, la conservation et les utilisations ultérieures de ses renseignements personnels recueillis à des fins autorisées par la loi.

dépersonnalisation (de-identification)
Processus qui consiste à modifier les renseignements personnels de façon à en supprimer les identifiants dans une mesure appropriée aux circonstances. Les renseignements ainsi dépersonnalisés comportent un risque résiduel de repersonnalisation.

données (data)
Ensemble de valeurs liées à des sujets concernant des variables qualitatives ou quantitatives qui représente des faits, des statistiques ou des éléments d'information d'une manière formalisée et qui est propice à la communication, à la réinterprétation ou au traitement.

données agrégées (aggregated data)
En statistique, regroupement de données à partir de plusieurs mesures, ou en économie, regroupement de données de haut niveau qui sont composées d'une multitude ou d'une combinaison d'autres données plus individuelles. Dans un cas comme dans l'autre, les données agrégées devraient être généralisées de telle sorte qu'elles ne peuvent être liées à une personne, par exemple, en utilisant une fourchette d'âges, plutôt que des âges en particulier.

fichier de renseignements personnels (FRP) (personal information bank)
Document qui contient une description de renseignements personnels organisés et pouvant être extraits à l'aide du nom d'une personne ou d'un numéro, d'un symbole ou d'un autre identificateur propre à cette

personne. Les renseignements personnels décrits dans le FRP ont été, sont ou peuvent être utilisés à des fins administratives et ils relèvent d'une institution fédérale.

fins administratives (administrative purpose)
Destination de l'usage de renseignements personnels concernant un individu dans le cadre d'une décision le touchant directement (article 3). Cela comprend la plupart des utilisations des renseignements personnels pour confirmer l'identité (à des fins d'authentification et de vérification) et déterminer l'admissibilité des personnes aux programmes gouvernementaux.

fins non administratives (non-administrative purpose)
Destination de l'usage de renseignements personnels à une fin qui n'est pas liée à quelque processus décisionnel touchant directement l'individu. Il s'agit notamment de l'usage de renseignements personnels à des fins comme la recherche, les statistiques, la vérification et l'évaluation.

fonctionnaire désigné (designated official)
Personne désignée par une institution fédérale comme étant le signataire d'une EER qui aura la responsabilité administrative globale de l'EER et des annexes connexes.

numéro d'assurance sociale (NAS) (social insurance number [SIN])
Numéro utilisable comme numéro de dossier ou de compte ou pour le traitement des données, tel qu'il est défini au paragraphe 28.1 (3) de la *Loi sur le ministère de l'Emploi et du Développement social*. Pour l'application de l'alinéa 3 *c*) de la *Loi sur la protection des renseignements personnels*, le NAS étant un numéro d'identification, il est considéré comme un renseignement personnel.

programme ou activité (program or activity)
À des fins de collecte, d'utilisation ou de communication appropriées de renseignements personnels par les institutions fédérales visées par la politique, programme ou activité autorisé ou approuvé par le Parlement.

L’autorisation parlementaire est habituellement prévue par une loi fédérale ou par un règlement subséquent. L’autorisation parlementaire peut également prendre la forme d’une approbation des dépenses proposées dans le Budget principal des dépenses et autorisée par une loi de crédits. Sont également incluses dans cette définition toutes les activités menées dans le cadre de l’administration du programme.

renseignements personnels (personal information)
« Renseignements, quel que soit leur forme et leur support concernant un individu identifiable » (article 3). Voir l’article 3 de la *Loi sur la protection des renseignements personnels* pour obtenir d’autres informations.

renseignements personnels sensibles (sensitive personal information)
Même si pratiquement tous les renseignements personnels peuvent être sensibles dans certains contextes (par exemple, la communication de l’adresse domiciliaire d’un individu peut l’exposer à des risques tant sur le plan personnel que professionnel), certaines catégories de renseignements personnels sont considérées comme étant sensibles pour la totalité ou la majorité des personnes. Parmi ces renseignements, mentionnons les renseignements médicaux, les renseignements financiers, les antécédents criminels, ou des identificateurs utilisés à grande échelle, comme le numéro d’assurance sociale ou d’autres renseignements dont la communication pourrait porter préjudice à la personne concernée (par exemple, vol d’identité, fraude, trouble émotionnel, ou effets négatifs sur la carrière d’une personne, sa réputation, sa situation financière, sa sécurité, sa santé ou son mieux-être, etc.).

représentant autorisé (authorized representative)
Personne autorisée par le fonctionnaire désigné à exécuter les modalités particulières de l’entente et qui peut modifier les annexes de l’EER, sauf pour une nouvelle utilisation des renseignements personnels.

responsable de l’institution fédérale (head)
Ministre, dans le cas d’un ministère ou d’un ministère d’État. Dans tout autre cas, il s’agit de la personne désignée par le Décret sur la désignation

des responsables d'institutions fédérales (*Loi sur la protection des renseignements personnels*). Si aucune personne n'est désignée, le premier dirigeant de l'institution, quel que soit son titre.

usage compatible (consistent use)
Utilisation qui a un lien raisonnable et direct avec les fins pour lesquelles les renseignements ont été recueillis ou compilés. Cela signifie que les fins initiales et les fins proposées sont si étroitement liées que la personne s'attend à ce que les renseignements soient utilisés à des fins compatibles, même si l'usage n'est pas expressément indiqué.

Documents de référence et liens utiles

Lois fédérales

- *Loi sur l'accès à l'information*
- *Charte canadienne des droits et libertés*
- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la protection des renseignements personnels*
- *Règlement sur la protection des renseignements personnels*

Politiques, directives et guide

- Directive sur le gouvernement ouvert
- Directive sur l'évaluation des facteurs relatifs à la vie privée
- Directive sur les pratiques relatives à la protection de la vie privée
- Directive sur le numéro d'assurance sociale
- Directive sur la gestion de la sécurité
- Guide de gestion intégrée du risque
- Politique sur l'accès à l'information
- Politique sur la protection de la vie privée
- Politique sur les services et le numérique

Date de modification :

2023-08-03