Employment and Social Development Canada
Emploi et Développement social Canada
Canada

Audit des ententes d'échange de renseignements

Rapport

Janvier 2025

Direction générale d'audit interne et de gestion des risques d'entreprise

Audit des ententes d'échange de renseignements

Les formats en gros caractères, braille, MP3 (audio), texte électronique, et DAISY sont disponibles sur demande en commandant en ligne ou en composant le 1 800 O-Canada (1-800-622-6232). Si vous utilisez un téléscripteur (ATS), composez le 1-800-926-9105.

PDF
Nº de cat. Em20-200/2025F-PDF
ISBN : 978-0-660-75043-9

1. CONTEXTE

Emploi et Développement social Canada (EDSC – le Ministère) gère de nombreux programmes et partage un volume important de renseignements. La gestion des fonds de renseignements administratifs du Ministère (y compris les renseignements personnels) est un projet complexe. Les renseignements sont stockés physiquement et électroniquement dans de nombreux systèmes, secteurs de programmes, directions générales et bureaux régionaux à travers le pays. Les ententes d'échange de renseignements (EER) sont des protocoles d'entente concernant les renseignements personnels divulgués entre les parties[1]. Les EER sont essentielles pour permettre au Ministère de gérer efficacement l'échange de renseignements avec les différents intervenants.

1.1 Objectif de l'audit

Cet audit avait pour objectif de fournir à la haute direction une assurance sur les points suivants :

- la mesure dans laquelle les EER sont gérées efficacement;
- la mesure dans laquelle le processus d'EER est géré conformément aux politiques pertinentes du Secrétariat du Conseil du Trésor (SCT).

1.2 Portée

La portée de l'audit comprenait une approche globale de la gestion des EER, couvrant les ententes d'échange de renseignements, Info Source (informations sur les programmes et les fonds de renseignements administratifs) et d'autres éléments liés au processus des EER. Toutes les EER actuellement actives pour un processus ou un programme donné ont été incluses dans la portée. L'audit n'a pas permis d'évaluer ou d'examiner les versions antérieures des EER qui ont été remplacées depuis par des EER actualisées.

1.3 Méthodologie

L'audit a utilisé les méthodes suivantes :

- Revue de documentation et analyses;
- Analyse des données et tour d'horizon;
- Entrevues sur la gestion et les équipes;
- Revue de dossiers.

[1] Directive sur les pratiques relatives à la protection de la vie privée

2. RÉSULTATS DE L'AUDIT

2.1 Les rôles et responsabilités ne sont pas clairement définis, documentés et délimités pour tous les intervenants concernés

La Politique ministérielle sur la gestion de la protection des renseignements personnels (PMGPRP) définit les responsabilités des intervenants ministériels en ce qui concerne la gestion des EER. Bien que la PMGPRP mentionne le rôle de la Chef de la protection des renseignements en tant qu'autorité fonctionnelle du Ministère pour toutes les questions relatives à la protection des renseignements personnels, ce qui inclut la formulation de conseils faisant autorité et de directives fonctionnelles à l'intention de toutes les directions générales et régions d'EDSC, elle ne délimite pas le rôle de la Chef de la Direction générale de la Dirigeante principale des données (DGDPD) dans le processus d'EER.

Les intervenants ont exprimé une certaine confusion quant aux rôles, aux responsabilités et aux obligations de rendre compte de la Division de la gestion de la protection des renseignements personnels (DGPRP), supervisée par la Chef de la protection des renseignements personnels, et de la DGDPD. De nombreux intervenants et directions générales ont fait part de leur incertitude quant à la participation de la DGPRP et de la DGDPD aux différentes étapes de la création et de la gestion des EER.

Bien que la DGDPD ait exprimé son intérêt pour la mise en place d'activités et d'initiatives liées aux EER au cours des prochaines années, il n'existe actuellement aucune feuille de route ni aucun plan de mise en œuvre détaillé.

Recommandation

1. La DGPRP, en collaboration avec la DGDPD, devrait mettre à jour la politique ministérielle afin de définir les rôles, les responsabilités et l'obligation de rendre compte de tous les intervenants en ce qui concerne les activités de gestion, de suivi et de contrôle des EER.

Réponse de la direction

Nous sommes d'accord avec la recommandation.

La DGPRP, en collaboration avec la DGDPD, devrait mettre à jour la politique ministérielle concernant la protection des renseignements personnels et les instruments de gestion de l'information afin de clarifier les rôles, les responsabilités et les obligations redditionnelles de toutes les parties en ce qui concerne la gestion, le suivi et la surveillance des EER. Ces instruments complémentaires énonceront les rôles de la Chef de la protection des renseignements personnels, de la Dirigeante principale des données, de la DGPRP et de la DGDPD, compte tenu de leurs pouvoirs et mandats respectifs. De nouveaux produits et procédures seront élaborés pour communiquer ces paramètres de façon proactive aux intervenants.

2.2 Les documents d'orientation actuels ne sont pas conformes aux nouvelles exigences de la Directive sur les pratiques relatives à la protection de la vie privée du SCT et des documents d'orientation connexes

Le modèle standard d'EER du Ministère utilisé pour l'élaboration de nouvelles EER (un document clé pour la gestion des EER) a été mis à jour pour la dernière fois en 2016. Depuis lors, le SCT a publié un nouveau modèle d'EER au début de 2023 et des orientations actualisées en matière d'EER à la mi-2023. La DGPRP et la DGDPD ont conçu un modèle d'EER et des orientations actualisées, mais ces mises à jour ne sont pas encore terminées. Par conséquent, les

orientations et les modèles de soutien actuels du Ministère ne sont pas encore alignés sur les nouvelles orientations du SCT.

La DGPRP a progressivement augmenté le nombre d'orientations relatives aux EER fournies aux propriétaires de programmes d'EER, ce qui inclut diverses présentations sur l'intranet du Ministère. Toutefois, les formations internes ciblées portant expressément sur les EER sont peu nombreuses. La plupart des coordonnateurs de direction générale en matière d'EER interrogés ne connaissent pas les documents d'orientation relatifs aux EER disponibles. Les directions générales ont manifesté un vif intérêt pour une formation générale (et ciblée) accrue, qui pourrait contribuer à atténuer les risques liés à l'échange de renseignements.

Recommandation

2. La DGPRP devrait achever les mises à jour du modèle et des orientations ministériels en matière d'EER pour les harmoniser avec la nouvelle politique et les nouvelles orientations du SCT.

Réponse de la direction

Nous sommes d'accord avec la recommandation.

La DGPRP et la DGDPD collaborent à l'élaboration de nouveaux modèles d'EER et de nouveaux documents d'orientation qui concordent avec ceux publiés par le SCT en 2023. Ces instruments seront conformes aux changements apportés à la *Politique sur la protection de la vie privée* du SCT en octobre 2024. Il y aura d'autres mises à jour des modèles et directives d'EDSC concernant les EER pour les harmoniser avec le cadre de gouvernance susmentionné et la directive ministérielle prévue.

Les nouvelles exigences relatives aux EER seront communiquées aux intervenants et aux clients à l'interne. Les produits de formation de la DGPRP sur les EER seront adaptés, et de nouvelles formations, en personne ou en ligne, seront conçues et proposées à une fréquence accrue.

2.3 Le Ministère conserve des EER datant de diverses périodes, dont beaucoup ne sont ni régulièrement examinés ni mises à jour, ne comportent pas de date d'expiration et manquent certaines données essentielles, telles que les détails sur les méthodes d'échange

La *Directive sur les pratiques relatives à la protection de la vie privée* du SCT et les orientations qui s'y rapportent :

- définit les EER comme étant «un protocole d'entente écrit qui définit les modalités selon lesquelles les renseignements personnels sont divulgués entre les parties»;
- précise qu'il convient de mettre en place des EER assorties de garanties appropriées avant toute divulgation de renseignements personnels;
- fournit des renseignements sur les domaines que les EER devraient aborder (c'est-à-dire l'objectif des EAR, la conservation et l'élimination des renseignements, les garanties générales, les périodes d'examen, les dates d'expiration, etc.).

Il a été constaté que de nombreuses EER du Ministère ne contenaient pas de périodes d'examen, de dates d'expiration ou de détails suffisants dans la section relative à la méthode d'échange.

Les récentes mises à jour de la *Directive sur les pratiques relatives à la protection de la vie privée* du SCT exigent que chaque service mette à la disposition du public des résumés de toutes les EER par le biais d'une mise à jour annuelle de l'«Info

Source» en ligne de l'institution. Il existe un risque que le Ministère répertorie les EER expirées (ou inactives et n'ayant plus de raison d'être) sur l'Info Source publique.

Recommandation

3. La DGPRP devrait établir un plan de mise à jour des EER pour les rendre conformes aux exigences du SCT et accélérer la mise à jour des EER considérées comme présentant le risque le plus élevé.

Réponse de la direction

Nous sommes d'accord avec la recommandation.

La DGPRP, en collaboration avec la DGPDP, examinera chacune des quelque 1 000 EER dans le dépôt de la DGPDP et évaluera les risques qui s'y rattachent. Les analystes de la protection des renseignements personnels repéreront et évalueront les manquements aux lois pertinentes ainsi qu'aux exigences des politiques du SCT et d'EDSC concernant les renseignements personnels.

Les EER qui présentent un risque élevé d'atteinte à la vie privée seront classées par ordre de priorité et la direction générale ou le programme responsable sera avisé afin de pouvoir procéder à une mise à jour. S'il n'est pas possible de faire une mise à jour, la direction générale ou le programme responsable devra préparer et exécuter un plan de gestion des risques, plan qui devra être approuvé par la Chef de la protection des renseignements personnels. La DGPRP supervisera la mise en œuvre de ces plans ainsi que la gestion des ententes visées.

2.4 La DGPRP et la DGDPD ne surveillent pas suffisamment les activités d'échange liées aux EER et n'informent pas la gouvernance sur les activités d'échange

Le référentiel d'EER, créé en 2016 et géré par la DGDPD, est le principal outil de gestion des EER du Ministère. La DGDPD est chargée de veiller à son exhaustivité et à sa mise à jour continue. La DGPRP limite son rôle aux activités directement liées à la création des documents relatifs aux EER et ne participe pas activement à la gestion ou à l'exécution des EER après qu'elles ont été conclues et signées par le propriétaire du programme à l'échelon des sous-ministres adjoints.

La plupart des intervenants des directions générales interrogés ont estimé que le référentiel d'EER n'était ni convivial ni particulièrement efficace pour la gestion des EER. En outre, le Ministère ne dispose pas d'une méthode détaillée, cohérente et structurée pour évaluer et noter les degrés de risque des EER, ce qui a une incidence sur la capacité à déterminer les EER qui pourraient nécessiter un examen plus approfondi de la part du Comité des données et de la protection des renseignements personnels (CDPRP).

En outre, il n'existe pas de fonction de contrôle des activités d'échange de renseignements liées aux EER pour confirmer le respect des exigences des EER et des pratiques adéquates de protection de la transmission et de l'accès aux renseignements. En outre, le rôle de surveillance de la CDPRP dans le processus lié aux EER n'est pas défini dans son mandat.

Recommandation

4. La DGPRP devrait renforcer l'approche de l'évaluation des degrés de risque des EER, entreprendre des activités de surveillance des EER fondées sur les risques afin de valider l'adéquation des pratiques d'échange de renseignements et informer périodiquement la gouvernance des résultats.

Réponse de la direction
Nous sommes d'accord avec la recommandation.

La DGPRP a évalué les risques des EER moins structurées ou plus informelles que celles normalement visées par les évaluations des facteurs relatifs à la vie privée. Elle mettra en œuvre un processus d'évaluation pour l'utilisation de renseignements personnels à des fins administratives et des analyses du protocole de protection des renseignements personnels qui comprennent des évaluations des risques pour les utilisations non administratives de renseignements personnels. Grâce à ces approches, la DGPRP améliorera la structure, la rigueur et la cohérence du processus d'évaluation des risques liés à la protection des renseignements personnels dans le contexte des EER. Les directions générales ou les programmes responsables devront élaborer et mettre en œuvre des plans de gestion des risques.

La DGPRP, en collaboration avec la DGDPD, mettra en place un nouveau programme de surveillance des EER. La DGPRP recueillera périodiquement des renseignements sur la mise en œuvre et la gestion de chaque EER d'EDSC afin d'évaluer les mesures de contrôle adoptées pour la gestion des renseignements personnels et des ententes, notamment dans le but de déterminer s'il y a de nouveaux risques à atténuer. Les EER seront priorisées en fonction du risque et au moyen d'une sélection aléatoire.

Les résultats de ces examens seront soumis au CDPRP et à la haute direction d'EDSC. Le CDPRP a pour mandat d'assurer la surveillance des processus de gestion des risques qui concernent les données et les renseignements personnels contrôlés par le Ministère, y compris la surveillance des risques, la mise en œuvre de stratégies d'atténuation des risques et l'examen des questions qui pourraient poser un risque important pour le Ministère.

Recommandation
5. La DGDPD, en collaboration avec la DGPRP, devrait élaborer un plan de mise en œuvre pour les améliorations requises du référentiel d'EER, ainsi que pour toute autre amélioration prévue.

Réponse de la direction

Nous sommes d'accord avec la recommandation.

La DGDPD travaille actuellement à une refonte du dépôt des EER. Nous planifions actuellement sa migration vers une plateforme moderne. Les métadonnées du dépôt sont examinées et ajustées, au besoin, pour appuyer la conformité aux lois et aux politiques et améliorer la prise de décisions. La DGDPD collaborera avec la DGPRP pour que les changements au dépôt facilitent la surveillance et le suivi des EER.

3. Conclusion

En conclusion, le Ministère se heurte à des difficultés pour gérer efficacement les EER conformément aux exigences du SCT. Les rôles et responsabilités des intervenants ne sont pas clairement définis, les documents d'orientation sont obsolètes et de nombreuses EER ne font pas l'objet d'examens réguliers, ne comportent pas de date d'expiration et ne contiennent pas de détails essentiels sur les méthodes d'échange de données. En outre, le suivi des activités liées aux EER n'est pas assuré par la DGPRP ou la DGDPD. L'amélioration de la documentation, la mise à jour des orientations et le renforcement de la surveillance seront essentiels pour améliorer le respect des règles et la protection des données.

4. DÉCLARATION D'ASSURANCE

Selon notre jugement professionnel, des procédures d'audit suffisantes et appropriées ont été mises en œuvre et des éléments de preuve ont été recueillis pour étayer l'exactitude des conclusions tirées et contenues dans le présent rapport. Les conclusions sont fondées sur les observations et les analyses effectuées au moment de l'audit. Les conclusions ne s'appliquent qu'à l'Audit des ententes d'échange de renseignements. Les éléments de preuve ont été recueillis conformément à la *Politique sur l'audit interne* du Conseil du Trésor et aux *normes internationales pour la pratique professionnelle de l'audit interne*.

ANNEXE A : ÉVALUATION DES CRITÈRES DE L'AUDIT

Critères d'audit	Cote
Rôles et responsabilités	Contrôles clés manquants : Exposition accrue aux risques
Orientation et soutien	Contrôlé, mais devrait être renforcé : Exposition moyenne aux risques
Ententes et expertise	Contrôles clés manquants : Exposition accrue aux risques
Direction et supervision	Contrôlé, mais devrait être renforcé : Exposition moyenne aux risques

ANNEXE B : GLOSSAIRE

CDPRP	Comité des données et de la protection des renseignements personnels
DGDPD	Direction générale de la dirigeante principale des données
DGPRP	Division de la gestion de la protection des renseignements personnels
EER	Ententes d'échange de renseignements
EDSC	Emploi et Développement social Canada
PMGPRP	Politique ministérielle sur la gestion de la protection des renseignements personnels
SCT	Secrétariat du Conseil du Trésor