**Protection des renseignements personnels dans le cadre du travail à distance**

**Contexte**

Le présent document d’information vise à aider les fonctionnaires à protéger les renseignements personnels et à prévenir les atteintes à la vie privée lorsqu’ils travaillent à distance.

Le travail à distance est devenu la nouvelle norme pour de nombreux fonctionnaires. Bien que cela offre de nouvelles possibilités d’explorer davantage de méthodes de travail numériques, le travail à distance a changé la façon dont les fonctionnaires créent et gèrent l’information et collaborent avec les autres. Les changements ont posé de nouveaux défis aux processus établis en milieu de travail, aux pratiques de gestion de l’information, à la prestation de services et à la collaboration interne qui sont habituellement protégés dans le cadre de la sécurité des installations et des environnements réseau du gouvernement du Canada.

La *Loi sur la protection des renseignements personnels* et les politiques fédérales en matière de protection des renseignements personnels exigent que les institutions fédérales et les employés protègent les renseignements personnels dont ils sont responsables. Cette mesure s’applique au travail à distance. De plus, en vertu de la *Politique sur les services et le numérique*, la protection des renseignements personnels doit être prise en compte dans tout plan ou toute stratégie de gestion des renseignements ou des données d’un ministère.

Les renseignements fournis ci-dessous tiennent lieu de conseils et de ressources utiles pour protéger les renseignements personnels et prévenir les atteintes à la vie privée dans le cadre du travail à distance.

|  |
| --- |
| **Atteintes à la vie privée**Par « atteinte à la vie privée », on entend la création, la collecte, l’utilisation, la communication, la conservation ou l’élimination inappropriée ou non autorisée de renseignements personnels.**Que faire si vous soupçonnez qu’il y a eu atteinte à la vie privée?**Vous devez signaler toute atteinte présumée à la vie privée au bureau de l’AIPRP de votre institution et suivre les plans et procédures de votre institution en matière de gestion des atteintes à la vie privée. Le bureau de l’AIPRP sera en mesure de vous fournir des renseignements plus précis et d’indiquer les prochaines étapes.Le tableau ci-dessous présente des scénarios et des points à considérer pour vous orienter dans la prévention et la gestion des atteintes potentielles à la vie privée lorsque vous travaillez à distance. |

**Références connexes :**

* [Politique intérimaire sur la protection de la vie privée](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510)
* [Politique sur la sécurité du gouvernement](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578)
* [Directive sur les services et le numérique](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601)
* [Lignes directrices sur les atteintes à la vie privée](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26154)

D’autres liens spécifiques au contenu se trouvent directement dans le texte ci-dessous.

|  |
| --- |
| **Scénario 1 :** Dans le contexte du travail à distance, les employés peuvent utiliser de nouveaux outils de collaboration numérique ou de productivité pour se connecter avec d’autres ou faire progresser leur travail.  |
| ***Points à considérer****Il est important de souligner que certains renseignements personnels sur les fonctionnaires tels que leur nom, titre de poste, classification, adresse courriel professionnelle et numéro de téléphone professionnel ne sont pas considérés comme des renseignements personnels protégés par la Loi sur la protection des renseignements personnels.* *Vous trouverez des renseignements et des conseils importants sur l’utilisation des outils de collaboration dans les* [*Conseils pour l’utilisation sécuritaire des outils de collaboration*](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gcpedia.gc.ca%2Fgcwiki%2Fimages%2F4%2F4e%2FOrientation_sur_la_facilitation_de_l%25E2%2580%2599acc%25C3%25A8s_aux_services_Web.pdf&data=04%7C01%7C%7C5bd4a141d7fd4dee86e008d8a03cd8b3%7C2f436130bd914cfbb216a9127020e559%7C0%7C0%7C637435530476800587%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=kr7vyrajwxRcDGVx6o7PjFxVBgn1%2BVxXOTRBvUxnuk0%3D&reserved=0) *et sur le* [*Wiki sur le travail à distance sécurisé*](https://wiki.gccollab.ca/Travail_%C3%A0_distance_s%C3%A9curis%C3%A9)*.* |
| ***Q : Dois-je fournir des renseignements personnels tels que mon numéro de téléphone personnel ou mon adresse courriel personnelle afin d’utiliser les outils de collaboration numérique sur en milieu de travail?***R : Non. Les outils de productivité ou de collaboration utilisés dans le cadre de vos responsabilités et fonctions en tant que fonctionnaire ne devraient nécessiter que des coordonnées professionnelles. ***Q : Lorsque j’utilise des outils de collaboration ou des outils de réunion virtuelle, je peux avoir besoin de discuter de renseignements personnels sensibles sur une personne identifiable. Est‑ce approprié?*** R : Il est souvent nécessaire de discuter de renseignements personnels sensibles dans le cadre de vos responsabilités et fonctions en tant que fonctionnaire. Par exemple, les employés chargés des relations de travail discutent de renseignements personnels sensibles avec les gestionnaires. Lorsque vous utilisez des outils numériques pour communiquer des renseignements personnels, avant d’utiliser un nouvel outil, communiquez avec les responsables de votre messagerie instantanée, de la sécurité et de la protection de la vie privée pour vous assurer que cet outil est adapté à votre situation.  ***Q : Je suis invité à utiliser un outil de visioconférence. Je ne suis pas à l’aise de partager mon image vidéo. La Loi sur la protection des renseignements personnels comporte-t-elle des exigences dont je devrais être conscient?*** R : Une image est un renseignement personnel lorsqu’elle concerne un individu identifiable et est enregistrée sous quelque forme que ce soit. Par conséquent, si votre image est enregistrée par l’outil, elle doit être protégée conformément à la *Loi sur la protection des renseignements personnels* et aux instruments de politique connexes. Si vous n’êtes pas à l’aise avec les fonctionnalités vidéo d’un outil de réunion virtuelle, vous devez d’abord discuter de vos préoccupations avec votre gestionnaire. Il sera en mesure de vous fournir plus d’assistance sur la meilleure voie à suivre. Souvent, les outils de réunion virtuelle ont des fonctionnalités qui permettent la participation sans utiliser la fonction vidéo. ***Q : J’ai installé des assistants à domicile (Google, Alexa, etc.) partout toute ma maison, puis-je encore faire du télétravail?***R : Oui, mais vous devez prendre des précautions contre la divulgation inappropriée de renseignements personnels à tout moment lorsque vous travaillez à distance. Vous pouvez par exemple supprimer ou désactiver le dispositif d’écoute passive de votre espace de travail. La *Loi sur la protection des renseignements personnels* et les politiques gouvernementales en matière de sécurité et de confidentialité exigent la protection des renseignements personnels et les dispositifs d’écoute passive pourraient poser un risque supplémentaire. Veuillez communiquer avec le bureau de l’AIPRP et le chef de la sécurité de votre institution pour obtenir de plus amples renseignements. Vous pouvez également visiter le site Web [Pensez cybersécurité](https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-appareils/televiseurs-et-appareils-intelligents) pour obtenir des conseils sur la sécurisation de vos appareils en ligne à la maison.  |

|  |
| --- |
| **Scénario 2 :** Dans le contexte du travail à distance, les employés peuvent apporter des documents papier contenant des renseignements personnels sur une personne identifiable à la maison. |
| ***Points à considérer****Pour prévenir les atteintes à la vie privée dans votre environnement de télétravail, vous devez aménager un espace dédié auquel vous pouvez restreindre l’accès des visiteurs occasionnels (par exemple : membres de la famille, invités, travailleurs). Les documents contenant des renseignements personnels doivent être stockés de manière appropriée et, lorsqu’ils ne sont plus nécessaires, détruits de manière appropriée. Veuillez consulter la* [*Directive sur la gestion de la sécurité — Annexe J : Norme sur la catégorisation de sécurité*](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32614) *ou communiquer avec les bureaux de gestion et de sécurité de l’information de votre institution pour obtenir de plus amples renseignements.* *Gardez à l’esprit que, conformément à la Directive sur les services et le numérique, les DPI doivent s’assurer que les* ***systèmes numériques******sont l’option privilégiée*** *pour créer, saisir et gérer des renseignements.* |
| ***Q : Quelle est la désignation de sécurité attribuée aux renseignements personnels?*** R : Cela dépend de la nature des renseignements personnels. Par exemple, les coordonnées d’une personne identifiable sont généralement désignées comme Protégé A, tandis que les coordonnées d’une personne identifiable qui est un informateur confidentiel des services d’application de la loi sont généralement considérées comme Protégé C.  Indépendamment de la désignation de sécurité attribuée aux renseignements personnels, toute création, collecte, utilisation, communication, conservation ou élimination inappropriées des renseignements personnels constitue une atteinte à la vie privée.***Q : Comment connaître les techniques appropriées pour sécuriser et transporter des dossiers papier contenant des renseignements personnels?***R : La personne la mieux indiquée pour vous fournir des renseignements spécifiques au stockage, au transport, à la transmission et à la destruction sécurisés de documents lorsque vous travaillez à distance est votre gestionnaire. À défaut, vous pouvez communiquer avec les bureaux de gestion et de sécurité de l’information de votre institution. La mallette de transport, la serrure, le mode de transport et le stockage à domicile devront être appropriés à la désignation de sécurité attribuée aux renseignements personnels. Le [lien](https://www.canada.ca/fr/gouvernement/fonctionpublique/covid-19/gestion-donnees-gouvernementales-travail-distance.html) suivant propose également des conseils supplémentaires sur la gestion des données dans le contexte du travail à distance. |

|  |
| --- |
| **Scénario 3 :** Dans le contexte du travail à distance, les employés peuvent avoir besoin de fournir des services d’une nouvelle manière, tout en continuant à protéger les renseignements personnels. |
| ***Points à considérer****Pour prévenir les atteintes à la vie privée lors de la prestation de services à distance, vous devez tenir compte de l’incidence du changement de modèle de prestation sur le flux (création, collecte, utilisation, communication, conservation, élimination) des renseignements personnels et sa gestion, et collaborer avec le bureau de l’AIPRP de votre institution pour déterminer si ces changements nécessitent une évaluation des facteurs relatifs à la vie privée. Veuillez consulter les exigences de la* [*Directive intérimaire sur l’évaluation des facteurs relatifs à la vie privée*](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18309) *ou communiquer avec le Bureau de l’accès à l’information et de la protection des renseignements personnels de votre institution pour obtenir de plus amples renseignements.*  |
| ***Q : Comment le changement de mode de prestation de services, soit d’un modèle en personne à un modèle à distance, affecte-t-il la gestion des renseignements personnels?*** R : Cela dépend de l’institution ainsi que du programme ou du service et des outils utilisés dans le cadre du processus. Par exemple, certains services peuvent utiliser de nouvelles technologies ou recourir à des fournisseurs tiers pour fournir des renseignements au destinataire du service. Cela pourrait entraîner une création, une utilisation, une communication, une conservation ou une élimination nouvelle et éventuellement non autorisée de renseignements personnels, c’est-à-dire une atteinte à la vie privée. Par exemple, si un tiers conservait une copie des données utilisées dans le cadre du service à ses propres fins commerciales, cela pourrait être considéré comme une conservation ou une utilisation non autorisée de renseignements personnels entraînant une atteinte à la vie privée. De même, un nouvel outil ou une nouvelle technologie pourrait nécessiter la collecte de renseignements personnels supplémentaires. Si elle n’est pas directement liée au programme ou à l’activité, cette nouvelle collecte pourrait constituer une atteinte à la vie privée. Pour évaluer les changements apportés aux processus opérationnels et leur incidence sur la gestion des renseignements personnels, les programmes de prestation de services devraient collaborer avec les bureaux de gestion de l’information et les bureaux de l’AIPRP correspondants pour déterminer si une évaluation des facteurs relatifs à la vie privée est nécessaire.***Q : Comment savoir si les nouveaux changements apportés à un processus opérationnel sont conformes aux exigences en matière de protection des renseignements personnels?******R :*** Les exigences en matière de protection des renseignements personnels sont énoncées dans la *Loi sur la protection des renseignements personnels*, les politiques du SCT en matière de protection des renseignements personnels et les lois et politiques propres à chaque institution. Veuillez collaborer avec votre bureau de gestion de l’information et de l’AIPRP pour discuter de tout changement aux processus opérationnels qui ont des répercussions sur la gestion des renseignements personnels afin de garantir que ceux-ci continueront d’être protégés.  |

|  |
| --- |
| **Scénario 4 :** Les employés qui travaillent à distance doivent s’assurer qu’ils enregistrent les documents dans les référentiels ministériels appropriés. |
| ***Points à considérer****La conservation et l’élimination inappropriées des renseignements personnels peuvent entraîner des atteintes à la vie privée. Pour éviter que cela ne se produise dans votre environnement de travail à distance, vous devez vous assurer que vous enregistrez les documents ayant une valeur opérationnelle dans le référentiel ministériel approuvé à cet effet. Il s’agit notamment de les classer de manière appropriée selon votre plan de classification ministériel, d’attribuer la désignation de sécurité appropriée à chaque document et de vous assurer que le référentiel ministériel est approuvé pour stocker, au minimum, les documents auxquels la même désignation est attribuée. Veuillez consulter la* [*Directive sur les services et le numérique*](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601) *ou communiquer avec les bureaux de gestion et de sécurité de l’information de votre institution pour obtenir de plus amples renseignements.* |
| ***Q : Puis-je enregistrer des documents contenant des renseignements personnels localement sur mon ordinateur de travail lorsque je travaille à distance?*** R : Non. Votre ordinateur de travail n’est pas un référentiel ministériel officiel. Il peut arriver que ce soit nécessaire de le faire, mais cela ne devrait se produire que lorsque cela est nécessaire et pour une période limitée. Par exemple, si vous perdez la connectivité réseau et devez sauvegarder le document, l’enregistrement local est autorisé à condition que lorsque vous vous reconnectez au réseau, le document soit enregistré dans le référentiel approprié.  ***Q : Existe-t-il des référentiels électroniques spéciaux dans lesquels enregistrer des renseignements personnels?***R : Cela dépend. Les renseignements personnels peuvent être enregistrés dans n’importe quel référentiel ministériel électronique si ce dernier est approuvé pour la désignation de sécurité du document et s’il satisfait par ailleurs aux exigences en matière de gestion de l’information du gouvernement du Canada. Dans la plupart des cas, les renseignements personnels sont correctement enregistrés dans le référentiel approuvé. À titre d’exception, il peut arriver que la désignation de sécurité attribuée aux renseignements personnels dépasse le niveau d’approbation du référentiel. Par exemple, lors de l’enregistrement de renseignements personnels concernant un informateur confidentiel. Les référentiels ministériels ne sont généralement pas appropriés dans ce cas, mais les renseignements en question doivent néanmoins être gérés comme un atout stratégique. Dans ce scénario, le bureau de gestion de l’information de votre institution peut vous fournir des instructions plus détaillées.  |