RAPPORT 2025-2026 PROTECTION DES RENSEIGNEMENTS PERSONNELS

SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE

MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

Bâtir l'avenir

Québec

RÉDACTION
Direction adjointe de la planification et de l'intégration au Service d'authentification gouvernementale du sous-ministériat adjoint à la sécurité de l'information gouvernementale et à la cybersécurité du ministère de la Cybersécurité et du Numérique

Si vous éprouvez des difficultés techniques ou si vous souhaitez obtenir une version adaptée du document, veuillez communiquer avec la Direction des communications :

Direction des communications
Ministère de la Cybersécurité et du Numérique
900, place D'Youville, 2e étage
Québec (Québec) G1R 3P7
Courriel : information@mcn.gouv.qc.ca

TABLE DES MATIÈRES

OBJECTIF DU RAPPORT

Le Rapport annuel 2025-2026 sur la protection des renseignements personnels du Programme Service québécois d'identité numérique (SQIN) répond aux obligations du ministère de la Cybersécurité et du Numérique (MCN) en matière de circulation et de protection des renseignements personnels qui sont requis à l'exécution de ses fonctions et de ses responsabilités spécifiquement à titre d'organisme public (OP) :

- Responsable de la gestion d'un projet en ressources informationnelles d'intérêt gouvernemental, soit le Programme Service québécois d'identité numérique (SQIN), incluant les projets qui le constituent. Ce rapport annuel est requis en application de l'article 10 de la *Loi favorisant la transformation numérique de l'administration publique* (RLRQ, chapitre T-11.003) (LFTNAP).

- Désigné comme source officielle de données numériques gouvernementales aux fins de l'identité numérique nationale. Ce rapport annuel est requis en application de l'article 12.17 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03) (LGGRI).

Ce rapport porte sur la période s'échelonnant du 1er avril 2025 au 31 mars 2026.

PROJET EN RESSOURCES INFORMATIONNELLES D'INTÉRÊT GOUVERNEMENTAL

Responsable

Le Secrétariat du Conseil du trésor a confié la responsabilité de la réalisation du Programme SQIN au Centre de services partagés du Québec, lequel a été aboli et remplacé par le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec, institué par la *Loi sur Infrastructures technologiques Québec* (RLRQ, chapitre I-8.4) en vigueur depuis le 1er septembre 2020.

La *Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions* (L.Q. 2021, chapitre 33) a été sanctionnée le 3 décembre 2021, ce qui abroge la *Loi sur Infrastructures technologiques Québec* (RLRQ, chapitre I-8.4). Le 1er janvier 2022, le MCN se voit confier les responsabilités qui étaient dévolues à Infrastructures technologiques Québec en vertu de sa loi constitutive.

Description

La mise en place du Programme SQIN vise à constituer une fondation, propulsant la personne citoyenne dans l'ère du numérique, lui procurant une identité numérique de confiance ainsi qu'en lui simplifiant l'accès aux services gouvernementaux. La sanction de la *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (L.Q. 2025, chapitre 26) donne au Programme SQIN les assises juridiques des concepts qu'il introduit (gestionnaire de l'identité numérique, portefeuille numérique, attestation numérique, MCN désigné source officielle de l'identité numérique nationale).

Ce programme comporte des projets en ressources informationnelles d'intérêt gouvernemental, dont le projet 1 « Accès bonifié aux prestations électroniques de services — Citoyens ». L'exécution du projet 1 a permis la mise en place du Service d'authentification gouvernementale, y compris la création du registre d'attributs d'identité gouvernemental (RAIG), pour l'identification et l'authentification des personnes en vue de leur donner accès aux prestations électroniques de services (PES) gouvernementales tout en contribuant à préserver à la fois l'intégrité et la confidentialité des renseignements personnels détenus par l'État.

Le RAIG, visé par le décret numéro 870-2022 du 25 mai 2022, devient le registre de l'identité numérique nationale (RINN) visé à l'article 10.7 de la *Loi sur le ministère de la Cybersécurité et du Numérique* (RLRQ, chapitre M-17.1.1) comme prévu à l'article 41 de la *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (L.Q. 2025, chapitre 26).

Objectifs et motivation du projet 1

Le projet 1 du Programme SQIN vise notamment à remplacer le service d'authentification clicSÉQUR pour permettre à un plus grand nombre de personnes citoyennes d'accéder plus facilement et de manière plus sécuritaire aux PES gouvernementales.

Les principaux objectifs du Service d'authentification gouvernementale sont les suivants :

- Fournir aux personnes utilisatrices un service d'authentification convivial, moderne, évolutif, extensible, sécuritaire et disponible;
- Simplifier le processus d'authentification et de vérification d'identité;
- Contribuer à la protection de l'intégrité et de la confidentialité des renseignements personnels détenus par l'État;
- Implanter un service unifié d'authentification gouvernementale qui contribue à la confiance du public dans les solutions technologiques de l'administration publique;

- Élargir le bassin de la clientèle potentielle aux PES gouvernementales.

L'institution du Service d'authentification gouvernementale vise aussi l'uniformisation des façons de faire des OP en matière d'authentification des personnes utilisatrices de leurs services en ligne.

Le Service d'authentification gouvernementale fait partie des moyens dont dispose l'État pour garantir à toute personne un accès sécurisé aux PES gouvernementales et lui permettre d'avoir un niveau de confiance élevé lors de ses interactions avec les OP.

Évolution du projet 1

La phase d'exécution du projet 1 « Accès bonifié aux prestations électroniques de services — Entreprises et Citoyens » du Programme SQIN a été autorisée par la prise du décret numéro 511-2020 du 13 mai 2020, et, depuis, le projet 1 a évolué. En effet, le gouvernement a autorisé la prise de plusieurs décrets relatifs au projet 1 notamment pour préciser les expérimentations, les changements significatifs sur la portée, dont le retrait du bloc « Accès bonifié aux prestations électroniques de services — Entreprises », et pour prolonger la phase d'exécution jusqu'au 13 mai 2025.

L'exploitation du Service d'authentification gouvernementale a commencé en décembre 2022, pendant l'exécution du projet 1. Son exploitation est sous la responsabilité du MCN.

Transition vers un service unifié d'authentification gouvernementale

Par la prise du décret numéro 1084-2024 du 10 juillet 2024, les OP visés à l'article 2 de la LGGRI seront tenus, au plus tard le 31 mars 2028, d'utiliser le Service d'authentification gouvernementale comme service d'authentification des personnes pour chacune de leurs PES. Il en est de même pour l'OP qui utilise déjà un autre service d'authentification des personnes. Cette exigence vise à faciliter les démarches des citoyennes et des citoyens, en plus de permettre l'utilisation du plein potentiel du Service d'authentification gouvernementale, dans une perspective d'optimisation de l'efficience gouvernementale de l'Administration en ligne.

SOURCE OFFICIELLE DE DONNÉES NUMÉRIQUES GOUVERNEMENTALES

Responsable

En vertu de l'article 10.4 de la *Loi sur le ministère de la Cybersécurité et du Numérique*, le MCN agit d'office comme source officielle de données numériques gouvernementales (SODNG) aux fins de l'identité numérique nationale. Dans l'exercice de ses fonctions à titre de SODNG, le MCN recueille, utilise ou communique des données numériques gouvernementales ou recueille auprès de toute personne des renseignements, incluant des renseignements personnels, lorsque cela est nécessaire.

Par la prise du décret numéro 870-2022 du 25 mai 2022, le gouvernement a désigné le MCN comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale. Ce décret est réputé pris conformément à l'article 10.6 de la *Loi sur le ministère de la Cybersécurité et du Numérique* (RLRQ, chapitre M-17.1.1), comme prévu à l'article 40 de la *Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (L.Q. 2025, chapitre 26).

Objectifs et motivation

Les OP recueillent et conservent les données d'identification nécessaires à leur prestation de services et en fonction de la clientèle qu'ils servent. Ainsi, chaque OP détient des renseignements d'identification qui concernent une portion des citoyennes et des citoyens. Conséquemment, ces renseignements sont, dans plusieurs cas, présents dans diverses bases de données gouvernementales.

À terme, le nombre de bases de données gouvernementales comprenant des renseignements d'identification sera réduit, ce qui entrainera une diminution du nombre de solutions permettant l'accès aux PES gouvernementales. Cela réduira les risques en matière de sécurité de l'information et d'atteinte à la vie privée et augmentera la cohérence gouvernementale au bénéfice des personnes concernées.

RENSEIGNEMENTS PERSONNELS IMPLIQUÉS

Les éléments suivants, prévus aux paragraphes 1 à 4 du premier alinéa de l'article 12.17 de la LGGRI, sont décrits dans l'annexe 1 « Vue d'ensemble de la circulation des renseignements personnels du Service d'authentification gouvernementale » :

1. Une description des renseignements personnels recueillis par le MCN ou qui lui ont été communiqués ainsi que leur provenance;

2. Les noms des OP à qui sont communiqués des renseignements personnels;

3. Une description des finalités pour lesquelles les renseignements personnels sont recueillis, utilisés ou communiqués;

4. Une description des moyens d'interaction et des modalités.

MESURES MISES EN PLACE POUR ASSURER LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les mesures propres à assurer la protection des renseignements personnels, prévues au paragraphe 5 du premier alinéa de l'article 12.17 de la LGGRI, sont énoncées dans l'annexe 2 « Mesures mises en place pour assurer la protection des renseignements personnels ».

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La personne responsable de la protection des renseignements personnels au MCN s'assure de la préparation, de la transmission et de la diffusion du rapport ainsi que de sa conformité avec les dispositions en vigueur.

La personne responsable de la protection des renseignements personnels au MCN, sur la base des informations et des documents reçus, atteste que l'ensemble des mesures appropriées identifiées ont été prises, sont en cours d'implantation ou en attente d'être mises en œuvre, afin d'assurer la protection des renseignements personnels. Les mesures prises font l'objet d'une surveillance et d'une révision en continu en vue de garantir le maintien d'une protection adéquate.

TRANSMISSION ET DIFFUSION

Comme prévu à l'article 10 de la LFTNAP, le MCN transmet ce rapport à la ministre de la Cybersécurité et du Numérique, de même qu'une copie à la Commission d'accès à l'information.

Comme prévu à l'article 12.17 de la LGGRI, le MCN transmet ce rapport à la Commission d'accès à l'information dans les 45 jours suivant la fin de l'année financière qu'il couvre. Conformément à l'article 12.18 de la même loi, une copie du rapport est également transmise au gestionnaire des données numériques gouvernementales et il est diffusé dans la section dédiée au MCN sur Québec.ca.

ANNEXE 1 – VUE D'ENSEMBLE DE LA CIRCULATION DES RENSEIGNEMENTS PERSONNELS DU SERVICE D'AUTHENTIFICATION GOUVERNEMENTALE

Note : Le portrait des renseignements personnels est mis à jour en continu. L'état de situation ci-dessous est celui du 31 mars 2026.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Nom Nom du mari pour les femmes mariées avant le 2 avril 1981 Date de naissance (DDN) Date du décès Adresse de résidence active Adresse de résidence future Indicateur de présence d'un répondant Numéro d'assurance maladie (NAM) Numéro d'assurance sociale (NAS)	RAMQ, Fichier d'inscription des personnes assurées (FIPA)	**Constitution et mise à jour du RAIG** Renseignements personnels communiqués au MCN pour la création et la mise à jour du RAIG, soit ceux nécessaires à l'identification des personnes pour leur donner accès aux PES gouvernementales. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : **Date du décès :** renseignement personnel communiqué au MCN pour permettre la désactivation d'un compte au Service d'authentification gouvernementale à la suite d'un décès. **Adresse de résidence :** renseignement personnel communiqué au MCN aux fins de correspondance. **Indicateur de présence d'un répondant :** renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence (identification d'une période pendant laquelle l'adresse peut être celle d'une tierce personne).	Décret numéro 870-2022 du 25 mai 2022. Décret numéro 1690-2022 du 26 octobre 2022 modifié par le décret 766-2023 du 3 mai 2023. Autorisation de mobilité des données numériques gouvernementales 2023-01 du gestionnaire de données numériques gouvernementales du 18 décembre 2023. Chargement initial des renseignements personnels en provenance du FIPA de la RAMQ vers le RAIG du MCN le 11 novembre 2022 visant uniquement les personnes âgées de 14 ans et plus inscrites au FIPA, à l'exception des personnes décédées et des personnes en processus de demande d'inscription pour qui la RAMQ n'a pas encore vérifié l'identité. Transmission de mises à jour de renseignements personnels [redacted] dans un canal sécurisé (aucune transmission inverse possible).

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Identifiant sectoriel de la RAMQ	Personnes qui utilisent le Service d'authentification gouvernementale	Spécifiquement pour les renseignements personnels suivants : **Nom, DDN, NAS, adresse de résidence** : renseignements personnels recueillis et utilisés aux fins d'identification des personnes en vue de leur donner accès au Portail d'inscription aux services de garde du ministère de la Famille.	Entente de collaboration entre l'OP partenaire et le MCN. Décret numéro 765-2023 du 3 mai 2023. Échanges en point de services autorisé. Interface d'échanges automatisés. Transaction informatique sécurisée.
[redacted]	[redacted]	[redacted]	[redacted]
Indicateur de changement d'adresse de résidence effectué par l'entremise du Service québécois de changement d'adresse (SQCA) Date de début et de fin de validité de l'adresse de résidence	RAMQ, FIPA	**Mise à jour du RAIG (gestion de l'adresse de résidence)** Spécifiquement pour les renseignements suivants : **Indicateur de changement d'adresse de résidence effectué par l'entremise du SQCA** : renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence [redacted] **Date de début et de fin de validité de l'adresse de résidence** : renseignement communiqué au MCN aux fins de gestion de l'adresse de résidence (identification d'une période de validité de l'adresse de résidence active).	Transmission de mises à jour de renseignement [redacted] dans un canal sécurisé (aucune transmission inverse possible).

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Adresse courriel Nom d'utilisateur Choix de langue	Personnes qui utilisent le Service d'authentification gouvernementale	**Création, modification et accès au compte au Service d'authentification gouvernementale** Renseignements personnels recueillis et utilisés, sur la base d'un consentement, pour la création, la modification ou l'accès au compte au Service d'authentification gouvernementale, et aux fins d'authentification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : **Adresse courriel et nom d'utilisateur :** renseignements personnels associés au mot de passe (premier facteur d'authentification). **Adresse courriel et choix de langue** : renseignements personnels utilisés aux fins de correspondance, notamment pour transmettre un code de sécurité (deuxième facteur d'authentification).	Règles relatives à l'assurance de l'identité numérique, prises par l'arrêté numéro 2024-03 du ministre de la Cybersécurité et du Numérique en date du 6 juillet 2024 modifiant l'arrêté numéro 2022-05 en date du 26 août 2022. Indication d'application numéro IA-SI-2022-001-OP du 4 octobre 2022. Interface d'échanges automatisés. Transactions informatiques sécurisées [redacted]. Génération automatique d'un code de sécurité. Transmission automatique par courriel d'un code de sécurité [redacted].
[redacted]	[redacted]	[redacted]	[redacted]

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Nom DDN NAM NAS Numéro d'avis de cotisation Numéro de référence de la carte d'assurance maladie Numéro de référence du permis de conduire	Personnes qui utilisent le Service d'authentification gouvernementale	**Processus d'identification en ligne** Renseignements personnels recueillis ou utilisés, sur la base d'un consentement, aux fins de l'identification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour les renseignements personnels suivants : [redacted] **Nom, DDN, NAS, numéro de référence de la carte d'assurance maladie ou numéro de référence du permis de conduire** : renseignements personnels recueillis et utilisés lorsque le mot de passe est oublié.	Règles relatives à l'assurance de l'identité numérique, prises par l'arrêté numéro 2024-03 du ministre de la Cybersécurité et du Numérique en date du 6 juillet 2024 modifiant l'arrêté numéro 2022-05 en date du 26 août 2022. Indication d'application numéro IA-SI-2022-001-OP du 4 octobre 2022. Interface d'échanges automatisés. Transactions informatiques sécurisées [redacted]

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Adresse de résidence Indicateur de présence d'un répondant Secret d'identification par la poste [redacted] Choix de langue	Personnes qui utilisent le Service d'authentification gouvernementale MCN	**Création et validation d'un secret d'identification par la poste** Renseignements personnels recueillis ou utilisés, sur la base d'un consentement, pour l'identification des personnes en vue de leur donner accès aux PES gouvernementales. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour les renseignements personnels suivants : **Indicateur de présence d'un répondant :** renseignement personnel utilisé aux fins de vérification de l'adresse. **Adresse de résidence et choix de langue :** renseignements personnels recueillis et utilisés aux fins de correspondance. **Secret d'identification par la poste** : renseignement [redacted] recueilli et utilisé afin de se substituer à un des secrets d'identification[1] pour l'identification des personnes. [redacted]	Interface d'échanges automatisés. Transactions informatiques sécurisées [redacted]. Génération d'un secret d'identification par la poste ayant une durée de validité limitée. [redacted]. Génération automatique d'une lettre.

[1] Les secrets d'identification comprennent un numéro d'avis de cotisation parmi les deux dernières années d'imposition (obligatoire sous réserve de l'utilisation d'un secret d'identification par la poste), le numéro de référence de la carte d'assurance maladie (optionnel) ou le numéro de référence du permis de conduire (optionnel).

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Seuls les renseignements personnels nécessaires parmi les suivants : Nom DDN NAM NAS Numéro d'immeuble Code postal ou numéro de case postale Adresse courriel	Personnes qui utilisent le Service d'authentification gouvernementale	**Processus d'identification en personne** Renseignements personnels recueillis et utilisés, sur la base d'un consentement, pour l'identification des personnes en vue de leur donner accès aux PES gouvernementales. Spécifiquement pour le renseignement personnel suivant : **Adresse courriel** : renseignement personnel utilisé pour vérifier que la personne est détentrice d'un compte au Service d'authentification gouvernementale et celui-ci est associé à un code de sécurité (deuxième facteur d'authentification).	Règles relatives à l'assurance de l'identité numérique, prises par l'arrêté numéro 2024-03 du ministre de la Cybersécurité et du Numérique en date du 6 juillet 2024 modifiant l'arrêté numéro 2022-05 en date du 26 août 2022. Indication d'application numéro IA-SI-2022-001-OP du 4 octobre 2022. Entente de collaboration entre l'OP partenaire et le MCN. Décret numéro 765-2023 du 3 mai 2023. Échanges dans un point de services autorisé. Interface d'échanges automatisés. Transactions informatiques sécurisées.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Renseignement(s) personnel(s) concernant les (2) pièces d'identité fournies, dont le type de pièce Type de la preuve d'adresse fournie, si applicable [redacted] Identifiant [redacted]	Personnes qui utilisent le Service d'authentification gouvernementale	**Vérification à postériori** Renseignement(s) personnel(s) recueilli(s) aux fins de vérification à postériori. [redacted]	Indication d'application numéro IA-SI-2022-001-OP du 4 octobre 2022. Entente de collaboration entre l'OP partenaire et le MCN. Décret numéro 765-2023 du 3 mai 2023. Échanges dans un point de services autorisé. Interface d'échanges automatisés. Transactions informatiques sécurisées.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Seuls les renseignements personnels nécessaires parmi les suivants : Nom DDN NAM Adresse courriel Adresse de résidence Renseignements en lien avec l'utilisation du compte au Service d'authentification gouvernementale Numéro de téléphone	Personnes qui utilisent le Service d'authentification gouvernementale	**Demande d'intervention au compte** Renseignements personnels recueillis utilisés, sur la base du consentement, pour l'identification des personnes en vue de traiter des demandes téléphoniques d'intervention au compte, soit pour bloquer ou réactiver un compte, modifier une adresse courriel ou signaler un problème technique. Au surplus de la finalité mentionnée ci-dessus et spécifiquement pour le renseignement personnel suivant : **Adresse courriel** : renseignement personnel utilisé aux fins de correspondance. Spécifiquement pour le renseignement personnel suivant : **Numéro de téléphone** : renseignement personnel utilisé aux fins de correspondance.	Communication téléphonique. Notifications transmises par courriel. Interface d'échanges automatisés [redacted] Transactions informatiques sécurisées [redacted].
Nom Adresse courriel Numéro de téléphone	Personnes qui formulent une plainte ou un commentaire Ministère de l'Emploi et de la Solidarité sociale (MESS) - Services Québec	**Plainte ou commentaire** Seuls les renseignements personnels fournis sont communiqués au MCN et utilisés, sur la base du consentement, aux fins de correspondance en vue de traiter une plainte ou un commentaire.	Entente de collaboration entre l'OP partenaire et le MCN. Communication téléphonique. Formulaire Web de plainte ou de commentaire. Transmission informatique sécurisée.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Identifiants [redacted] Adresse IP Ville et pays	Personnes qui utilisent le Service d'authentification gouvernementale MCN [redacted]	**Sécurité et soutien aux opérations** Renseignements personnels utilisés à des fins de sécurité et de soutien aux opérations [redacted] Spécifiquement pour les renseignements personnels suivants : **Ville et pays :** renseignements personnels inférés à partir de l'adresse IP.	[redacted] Transactions informatiques sécurisées [redacted].
Identifiants [redacted]	MCN [redacted]	**Statistiques de performance et de qualité** Renseignements personnels utilisés aux fins de production de statistiques en vue d'évaluer la performance et de mesurer la qualité du Service d'authentification gouvernementale, dans une perspective d'amélioration continue.	Transactions informatiques sécurisées [redacted]. Procédés techniques automatisés de dépersonnalisation.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	**Provenance**	**Description des finalités**	**Moyen d'interaction et modalité**
Adresse courriel	Ministère de la Famille (MFA) MCN	**Comparaison de données** Renseignement personnel communiqué au MCN et utilisé aux fins de comparaison de données pendant la période requise de transition pour le rattachement de certaines PES gouvernementales.	Indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024 Transfert sécurisé de fichier. Transactions informatiques sécurisées [redacted]
Identifiant [redacted] Adresse courriel ou nom d'utilisateur Langue d'affichage : FR (pour français) ou EN (pour anglais)	Personnes qui utilisent le Service d'authentification gouvernementale MCN	**Témoins de connexion** Renseignements personnels utilisés afin d'assurer le bon fonctionnement du site Web du Service d'authentification gouvernementale et afin d'améliorer et de personnaliser l'expérience utilisateur.	Transactions informatiques sécurisées [redacted].
Prénom et première lettre du nom de famille Adresse de résidence Renseignement concernant une situation de handicap	Personnes participantes	**Test d'utilisabilité** Renseignements personnels communiqués au MCN et utilisés aux fins du test d'utilisabilité du Service d'authentification gouvernementale.	Document contractuel entre le fournisseur de services et le MCN. Transmission informatique sécurisée. Procédé manuel de dépersonnalisation.

Renseignements personnels communiqués par le MCN			
Description des renseignements personnels	**Destinataire**	**Finalité**	**Moyen d'interaction et modalité**
Seuls les renseignements personnels nécessaires parmi les suivants : Nom DDN NAS [redacted] Numéro d'avis de cotisation ou numéro de référence de la carte d'assurance maladie ou numéro de référence du permis de conduire	OP partenaire : Agence du Revenu du Québec (RQ) Régie de l'assurance maladie du Québec (RAMQ) Société d'assurance automobile du Québec (SAAQ)	**Validation d'un secret d'identification** Renseignements personnels communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour la validation d'un secret d'identification.	Décret numéro 870-2022 du 25 mai 2022. Transmission dans un canal sécurisé.
Nom Adresse de résidence Secret d'identification par la poste	OP partenaire [redacted]	**Transmission d'un secret d'identification par la poste** Renseignements personnels communiqués, sur la base d'un consentement, aux fins du processus d'identification en ligne pour l'impression et l'expédition d'une lettre.	Entente de collaboration entre l'OP partenaire et le MCN. Transfert d'information sécurisé. Transmission [redacted] des lettres en lot. Impression des lettres sur papier. Lettres transmises par courrier postal.

Renseignements personnels communiqués par le MCN			
Description des renseignements personnels	**Destinataire**	**Finalité**	**Moyen d'interaction et modalité**
Seul(s) le(s) renseignements personnel(s) nécessaire(s) parmi les suivants : Nom DDN NAM NAS (complet ou partiel) Adresse de résidence Adresse courriel Identifiant(s) [redacted]	OP consommateur[2] : Agence du Revenu du Québec (RQ) Autorité des marchés financiers (AMF)* Commission des normes de l'éthique de la santé et de la sécurité au travail (CNESST) Conseil des arts et des lettres du Québec (CALQ) Curateur public Groupement des assureurs automobiles (GAA)* Ministère de l'Emploi et de la Solidarité sociale (MESS) Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs (MELCCFP)* Ministère de la Cybersécurité et du Numérique (MCN)* Ministère de la Famille (MFA)* Ministère de la Santé et des Services sociaux (MSSS)* Régie de l'assurance maladie du Québec (RAMQ)* Société d'assurance automobile du Québec (SAAQ)* Office de la protection du consommateur (OPC) Retraite Québec Santé Québec	**Identification de la personne** Renseignement(s) personnel(s) communiqué(s) aux fins d'identification de la personne en vue de lui donner accès à une PES gouvernementale.	Entente globale de service entre l'OP consommateur et le MCN (avec annexe spécifique). Indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024. Transmission dans un canal sécurisé.

[2] *OP ayant rattaché au moins une PES au Service d'authentification gouvernementale avant le 31 mars 2025.

Renseignements personnels communiqués par le MCN			
Description des renseignements personnels	**Destinataire**	**Finalité**	**Moyen d'interaction et modalité**
Seul(s) le(s) renseignements personnel(s) nécessaire(s) parmi les suivants : Nom DDN Adresse de résidence Adresse courriel	OP consommateur[3] : Autorité des marchés financiers (AMF)* Ministère de la Cybersécurité et du Numérique (MCN)* Ministère de la Famille (MFA)* Ministère de l'Environnement, de la Lutte contre les changements climatiques, de la Faune et des Parcs (MELCCFP)* Commission des normes de l'éthique de la santé et de la sécurité au travail (CNESST) Conseil des arts et des lettres du Québec (CALQ) Ministère de l'Emploi et de la Solidarité sociale (MESS)	**Remplissage automatisé** Renseignement(s) personnel(s) communiqué(s), sur la base du consentement, aux fins de remplissage automatique d'un formulaire d'inscription de la personne en vue de lui donner accès à une PES gouvernementale.	Entente globale de service entre l'OP consommateur et le MCN (avec annexe spécifique). Indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024. Transmission dans un canal sécurisé.

[3] *OP ayant rattaché au moins une PES au Service d'authentification gouvernementale avant le 31 mars 2025.

Renseignements personnels communiqués par le MCN			
Description des renseignements personnels	**Destinataire**	**Finalité**	**Moyen d'interaction et modalité**
Seul(s) le(s) renseignements personnels nécessaire(s) parmi les suivants : Nom DDN NAM NAS (complet) Adresse courriel	OP consommateur[4] : Autorité des marchés financiers (AMF)* Agence du Revenu du Québec (RQ) Ministère de la Famille (MFA) Ministère de l'Emploi et de la Solidarité sociale (MESS)	**Service à la clientèle** Renseignements(s) personnels(s) communiqué(s) aux fins de fourniture du service à la clientèle lorsqu'une erreur est détectée à l'occasion des travaux de rattachement au Service d'authentification gouvernementale d'une PES gouvernementale ou lors de l'accès à celle-ci.	Entente globale de service entre l'OP consommateur et le MCN (avec annexe spécifique). Indication d'application numéro IA-RI-2024-001-OP du 12 juillet 2024. Transmission dans un canal sécurisé.

[4] *OP ayant rattaché au moins une PES au Service d'authentification gouvernementale avant le 31 mars 2025.

ANNEXE 2 – MESURES MISES EN PLACE POUR ASSURER LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Responsabilité

Énoncé	Mesure mise en place
Règles de gouvernance encadrant les renseignements personnels détenus aux fins du Service d'authentification gouvernementale	Règles adoptées et accessibles au personnel du MCN concerné notamment : • Politique de confidentialité et de protection des renseignements personnels du MCN agissant à titre de source officielle de données numériques gouvernementales; • Procédure encadrant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels dans le cadre du Service québécois d'identité numérique. Règles de gouvernance encadrant les renseignements personnels transmises pour information à la Commission d'accès à l'information.
Formation et sensibilisation en matière de protection des renseignements personnels	Activités de formation et de sensibilisation offertes au personnel du MCN incluses au processus d'accueil et d'intégration pour tout nouvel employé (interne et externe) de la direction générale responsable du Programme SQIN. Formation obligatoire pour l'ensemble du personnel du MCN (protéger les renseignements personnels dans le secteur public de l'Académie de transformation numérique). Formation en gestion de risque pour les employés de l'équipe dédiée à la protection des renseignements du Programme SQIN. Révision en continu du plan de formation et de sensibilisation du MCN. Engagement de confidentialité et divulgation de conflits d'intérêts.
Ressources dédiées à la protection des renseignements personnels	Soutien-conseil en continu en matière de protection des renseignements personnels pour l'exécution du Programme SQIN et l'exploitation de ses produits et services. Désignation d'une personne responsable du suivi du déploiement des mesures d'atténuation des risques en matière de protection des renseignements personnels. Statutaire entre les équipes dédiées à la protection des renseignements personnels pour favoriser une saine coordination des activités et un partage de connaissances.
Ententes contractuelles avec les tiers sur l'encadrement, notamment la communication de renseignements personnels à	Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers, accessible au personnel concerné. Lignes directrices du Courtier infonuagique qui favorisent le respect des obligations relatives au maintien d'une protection adéquate pour l'hébergement des renseignements personnels. Audit externe réalisé par les fournisseurs en infonuagique préalablement à la signature d'un contrat, lequel vise le respect des plus hautes normes et des meilleures pratiques en matière

Énoncé	Mesure mise en place
l'extérieur du Québec	de sécurité de l'information et de protection, notamment celles des renseignements personnels. Clauses contractuelles qui prévoient les mesures de protection des renseignements personnels appliquées par les tiers, qui sont mandatés pour l'hébergement des données, notamment en matière de conservation de données de journalisation et de continuité du Service d'authentification gouvernementale advenant un sinistre majeur. Dépôt annuel, par les fournisseurs de services en infonuagique, de pièces justificatives requises auprès du MCN (ex. : rapport d'audit de sécurité de l'information basé sur le standard SSAE 16/SOC 2 Type II, attestations de destruction) pour démontrer leur conformité. Renforcement des mécanismes de vérifications du respect des exigences auprès des OP. Registre sectoriel en application de l'article 67.3 de la *Loi sur l'accès*, accessible au personnel concerné. Engagements des OP consommateurs prévus dans la fiche de services faisant partie intégrante de l'annexe spécifique du Service d'authentification gouvernementale dans l'entente globale de services du MCN.
Rapports en application des lois applicables	Rapport d'évaluation des facteurs relatifs à la vie privée (EFVP) publié conformément aux exigences de la LFTNAP et transmis selon les exigences de la LGGRI. Rapport annuel concernant les renseignements personnels recueillis, utilisés et communiqués aux fins du Service d'authentification gouvernementale et du Programme SQIN en application de la LFTNAP et de la LGGRI, publié et transmis selon les exigences des lois applicables.
Confiance du public dans le développement de solutions technologiques assurant le respect de la vie privée	Étude menée par la firme SOM au sujet du Service d'authentification gouvernementale (de septembre à décembre 2023) et mise en place d'un plan d'action (février 2024). Campagne de promotion au sujet du respect de la vie privée dans le cadre des activités du Service d'authentification gouvernementale (de juillet 2024 à mars 2025).
Outils d'évaluation, conformité et relations avec les OP consommateurs	Outil sectoriel d'évaluation et de validation pour la mise en œuvre des principes et des obligations en matière de protection des renseignements personnels, notamment pour la mise à jour de l'EFVP. Encadrement des demandes de communication de renseignements personnels vers les OP consommateurs incluant la formalisation des exigences en matière de protection des renseignements personnels requises dans le cadre de la démarche d'arrimage et le formulaire « Demande de communication de renseignements personnels du Service d'authentification gouvernementale vers l'OP ».

Détermination des finalités

Énoncé	Mesure mise en place
Finalités déterminées avant la collecte	Finalités de la collecte de renseignements personnels aux fins du Service d'authentification gouvernementale, déterminées par décret. Description de certaines activités (finalités) liées à l'identification et à l'authentification des personnes qui, aux fins du Service d'authentification gouvernementale, doivent être exécutées par les OP visés (indication d'application concernant les activités liées à l'identification et à l'authentification des personnes aux fins du Service d'authentification gouvernementale). Finalités pour lesquelles les renseignements personnels font l'objet d'une autorisation de mobilité par le gestionnaire des données numériques gouvernementales déterminées par décret. Finalités précisées dans les règles encadrant la gouvernance des renseignements personnels aux fins du Service d'authentification gouvernementale. Collecte des renseignements personnels en conformité avec les Règles relatives à l'assurance de l'identité numérique. Vue d'ensemble de la circulation des renseignements personnels impliqués dans le Service d'authentification gouvernementale présentant la description des finalités, accessible au personnel concerné. Interdiction d'utiliser les données du RINN à des fins de profilage comme prévu à l'article 10.7 de la *Loi sur le ministère de la Cybersécurité et du Numérique* (RLRQ, chapitre M-17.1.1).

Limitation de la collecte

Énoncé	Mesure mise en place
Légitimité à collecter les renseignements personnels aux fins déterminées	Désignation du MCN pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale par la prise du décret numéro 870-2022 du 25 mai 2022. Ce décret est réputé pris conformément à l'article 10.6 de la *Loi sur le ministère de la Cybersécurité et du Numérique* (RLRQ, chapitre M-17.1.1), comme prévu à l'article 40 de *la Loi concernant l'identité numérique nationale et modifiant d'autres dispositions* (L.Q. 2025, chapitre 26). Autorisation de mobilité des données numériques gouvernementales 2023-01 du gestionnaire de données numériques gouvernementales du 18 décembre 2023. Projet 1 « Accès bonifié aux prestations électroniques de services — Citoyen » du Programme SQIN désigné par le décret numéro 115-2028 du 14 février 2018 comme projet en ressources informationnelles d'intérêt gouvernemental.
Limitation de la collecte de renseignement personnel à ce qui	Évaluation de la nécessité de la collecte des renseignements personnels par rapport aux objectifs du projet 1 et à la solution proposée, et ce, avant la prise du décret numéro 870-2022 du 25 mai 2022.

Énoncé	Mesure mise en place
est nécessaire aux fins déterminées	Analyse approfondie des renseignements personnels nécessaires à l'exercice des attributions du MCN et à la mise en œuvre des processus d'authentification et d'identification des personnes qui souhaitent accéder à certaines PES gouvernementales par l'entremise du Service d'authentification gouvernementale. Champs à remplissage obligatoires prédéterminés dans les interfaces d'échanges automatisés sans possibilité d'ajouter d'autres renseignements personnels. Application de règles d'affaires pour valider le contenu de la saisie dans les champs à remplissage obligatoires prédéterminés.
Limitation de la collecte des renseignements personnels sensibles aux fins déterminées	Analyse de plusieurs combinaisons de renseignements personnels pour la réalisation du processus d'identification en ligne (ex. : nom, DDN et code postal; nom, DDN et nom de la mère) en tenant compte de l'existence des cas répertoriés de personnes ayant les mêmes noms, prénoms et DDN. Cette analyse a permis de démontrer que la combinaison du NAS et du NAM limite les risques de fraude par ingénierie sociale. Absence de pièce d'identité citoyenne québécoise (avec un numéro unique pour chaque citoyen) rendant difficile la corroboration des attributs de base (nom, prénom, DDN) auprès de la source de confiance et de les relier à une seule identité. Réalisation d'une analyse basée sur des identifiants existants démontrant qu'à part le NAS et le NAM, aucun autre identifiant présent dans les bases de données des OP ne peut donner l'assurance de l'unicité de l'identité d'une personne. [redacted] Combinaison du NAS et du NAM permettant de garantir la qualité des données en assurant en amont la fiabilité lors de l'identification en ligne de l'utilisateur et en aval lors de l'utilisation par l'ensemble des OP de la même information d'identité.

Protection dès la conception et par défaut

Énoncé	Mesure mise en place
Protection de la vie privée dès la conception	Réalisation d'une EFVP dès l'exécution d'un projet et lors de tout changement significatif.
Protection de la vie privée par défaut	Solution administrée selon les règles et les protocoles établis en vue d'assurer le plus haut niveau de confidentialité sans intervention des personnes. Paramétrage des fonctionnalités assurant le plus haut niveau de confidentialité sans intervention des personnes. Évaluation en continu des témoins de connexion utilisés aux fins du Service d'authentification gouvernementale. Désactivation par défaut du témoin de profilage (choix de langue). Informations fournies quant aux moyens pour activer ou refuser la localisation approximative (ville et pays) par l'entremise d'une

Énoncé	Mesure mise en place
	fenêtre informative et la Politique de confidentialité du Service d'authentification gouvernementale.

Consentement

Énoncé	Mesure mise en place
Consentement valide	Forme de consentement et méthode d'obtention appropriées à la sensibilité des renseignements personnels impliqués et adaptées aux personnes visées, au contexte et au type d'interface. Informations requises fournies au moment de la demande de consentement spécifiant notamment les finalités de l'utilisation ou de la communication concernée. Informations fournies concernant les conséquences d'un refus ou, le cas échéant, d'un retrait de son consentement suivant une demande facultative.
Exceptions au consentement	Obtention du consentement pour toute utilisation et communication de renseignements personnels aux fins déterminées, sauf exception prévue par la loi.
Documentation de l'obtention du consentement	Journalisation des évènements liés au consentement.
Retrait du consentement	Informations fournies concernant le droit de retrait du consentement.

Limitation de l'utilisation, de la communication et de la conservation

Énoncé	Mesure mise en place
Utilisation et communication aux seules fins déterminées	Limitation de la communication des renseignements personnels à des tiers situés à l'extérieur du Québec aux seules fins de prévention, de détection ou de diminution des impacts en cas d'atteinte ou de risque d'atteinte de confidentialité, de disponibilité ou d'intégrité. Analyse par les équipes dédiées à la protection des renseignements personnels des demandes d'utilisation et de communication de renseignements personnels, notamment à des fins compatibles (primaires et secondaires). [redacted] Limitation de l'utilisation secondaire des renseignements personnels aux seules fins statistiques avec dépersonnalisation dans le but d'évaluer la performance ou de mesurer la qualité du Service d'authentification gouvernementale dans une perspective d'amélioration continue. Limitation de la communication des renseignements personnels nécessaire au suivi d'une demande d'intervention au compte au Service d'authentification gouvernementale, seul le numéro de la demande est communiqué à la personne.

Énoncé	Mesure mise en place
	Registre sectoriel en application de l'article 67.3 de la *Loi sur l'accès*, accessible au personnel concerné.
Conservation des renseignements personnels pour la réalisation des fins déterminées	Calendrier de conservation du MCN et règle de conservation spécifique aux renseignements personnels détenus aux fins du Service d'authentification gouvernementale, établis par le MCN et approuvés par la Bibliothèque et Archives nationales du Québec (BAnQ). Toute modification apportée à un renseignement personnel au FIPA de la RAMQ entraine une modification du renseignement personnel concerné au RAIG (aucune conservation d'historique des renseignements personnels modifiés). Démarche d'élaboration du Plan de conservation et de destruction de renseignements personnels détenus aux fins du Service d'authentification gouvernementale. [redacted]

Exactitude

Énoncé	Mesure mise en place
Assurance de la qualité des renseignements personnels détenus aux fins du Service d'authentification gouvernementale	Informations fournies au regard de la responsabilité de la personne utilisatrice concernant la mise à jour de ses renseignements personnels par le biais de la Politique de confidentialité du Service d'authentification gouvernementale. Transmission de mises à jour des renseignements personnels [redacted] en provenance de la RAMQ dans un canal sécurisé (aucune transmission inverse possible). Analyse approfondie des processus de collecte en provenance d'une source de confiance avant la sélection de la source. Champ à remplissage prédéfini pour la saisie des renseignements dans les interfaces d'échanges automatisés du Service d'authentification gouvernementale. Règles d'affaires mises en application pour valider la qualité des données, comprenant des renseignements personnels (validation des formats et des contextes rendant notamment impossible l'inscription de certaines dates dans le futur dans le RAIG). Règles d'affaires mises en application pour la gestion des adresses de résidence en vue de la transmission de correspondance. Modification de l'adresse courriel et du mot de passe par l'entremise de la gestion de compte en ligne. Modification de l'adresse courriel par l'entremise d'une demande téléphonique d'intervention au compte. Journalisation des évènements liés à certaines modifications.

Sécurité

Énoncé	Mesure mise en place
Mesures de sécurité physiques, techniques et organisationnelles	Application des mesures pour assurer le caractère confidentiel de tous les renseignements personnels détenus aux fins du Service d'authentification gouvernementale qui prennent effet en amont de la collecte, notamment par le déploiement d'une infrastructure technologique sécuritaire. Indication d'application numéro IA-SI-2023-001-OP du 1er février 2023. Cadre normatif en matière de renseignements personnels, de sécurité de l'information et des conflits d'intérêts. Engagement de confidentialité et divulgation de conflits d'intérêts. Habilitations sécuritaires. Plusieurs types de mesures[5] appliquées pour protéger les renseignements personnels contre tout accès, utilisation, communication ou destruction non autorisés, toute perte ou toute autre forme d'atteinte à leur protection. Avis de sécurité de l'information émis par le MCN permettant d'identifier les mesures de sécurité appropriées pour protéger les renseignements personnels durant tout leur cycle de vie, incluant : • des mesures physiques, comme la restriction des accès aux locaux; • des mesures techniques ou technologiques, comme le chiffrement, le hachage ou de mécanismes d'authentification à facteurs multiples; • des mesures organisationnelles, comme l'adoption et l'application de règles en matière de sécurité de l'information et de protection des renseignements personnels, plan de reprise en cas de sinistre. Notifications transmises automatiquement par courriel aux personnes utilisatrices pour les informer de la survenance d'évènements liés au compte.
Mesures de sécurité proportionnelles au degré de sensibilité des renseignements personnels	Mesures de protection équivalentes à celles des règles particulières de protection du NAM et du NAS mises en place dans le cadre des expérimentations requises avant le déploiement du Service d'authentification gouvernementale. Mécanismes de contrôle et de vérification de l'efficacité et du respect des mesures de sécurité appliquées au Service d'authentification gouvernementale.
Règles de gouvernance concernant les incidents de sécurité, incluant les incidents de confidentialité	Directive sur la gestion des menaces, des vulnérabilités, des incidents de sécurité de l'information et des incidents impliquant des renseignements personnels, accessible au personnel concerné. Processus de signalement d'un incident en passant par les canaux de communication prédéterminés (téléphone ou courriel), accessible à l'ensemble du personnel du MCN.

[5] La liste complète des mesures applicables au Service d'authentification gouvernementale n'est pas accessible pour des raisons de sécurité.

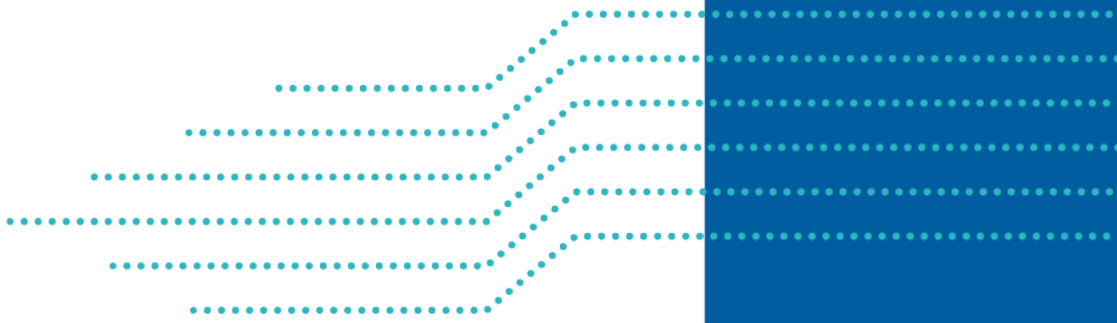
Énoncé	Mesure mise en place
	Processus de gestion des incidents de sécurité, qui relève du Centre organisationnel de cyberdéfense, prévoyant l'implication du responsable de la protection des renseignements personnels lorsque des renseignements personnels sont impliqués. Lorsque requis, les personnes concernées par un incident de confidentialité ainsi que la Commission d'accès à l'information sont avisées. Processus de signalement de compromission d'un compte au Service d'authentification gouvernementale, accessible au personnel concerné. Outils de surveillance utilisés pour la détection d'incident de sécurité. Actions correctrices déterminées en concertation avec les intervenants appropriés et réalisation des travaux dans les temps et les modalités prescrites selon la situation. Registre des incidents de confidentialité.

Transparence

Énoncé	Mesure mise en place
Informations fournies concernant les règles de gouvernance encadrant les renseignements personnels détenus aux fins du Service d'authentification gouvernementale	Plan de communication pour promouvoir les aspects de protection des renseignements personnels et de sécurité de l'information en lien avec le Service d'authentification gouvernementale.
Informations fournies concernant les pratiques de gestion et de protection des renseignements personnels détenus aux fins du Service d'authentification gouvernementale	Section dédiée au Service d'authentification gouvernementale accessible sur Québec.ca, dans laquelle des informations sont fournies au sujet de la création d'un compte et des documents requis aux fins du processus d'identification. Capsule vidéo présentant les processus de création d'un compte et d'identification, diffusée dans la section dédiée au Service d'authentification gouvernementale sur Québec.ca. Documents en lien avec la gestion des renseignements personnels détenus aux fins du Service d'authentification gouvernementale présentés de manière claire et compréhensible diffusés sur le site du Service d'authentification gouvernementale (Politique de confidentialité du Service d'authentification gouvernementale et Conditions d'utilisation du Service d'authentification gouvernementale). Informations requises fournies en personne ou au téléphone. Informations générales concernant le consentement accessibles dans le bandeau de bas de page du site Web du Service d'authentification gouvernementale.

Droits à l’égard des renseignements personnels

Énoncé	Mesure mise en place
Demandes d’accès et de rectification	Accessibilité pour consultation à certains renseignements personnels détenus aux fins du Service d’authentification gouvernementale par l’entremise de la gestion de compte en ligne. Politique de confidentialité du Service d’authentification gouvernementale détaillant les droits d’accès aux renseignements personnels et de rectification, laquelle est publiée sur le site du Service d’authentification gouvernementale. Procédure et processus de traitement des demandes d’accès et de rectification des renseignements personnels en lien avec le Service d’authentification gouvernementale, laquelle est accessible au personnel concerné.
Plainte ou commentaire concernant la gestion des renseignements personnels	Moyens pour formuler une plainte ou un commentaire concernant la gestion des renseignements personnels : téléphone, formulaire électronique transmis par courriel ou par la poste (Politique de confidentialité du Service d’authentification gouvernementale). Politique ministérielle de gestion des plaintes et des commentaires. Politique et processus de gestion des plaintes et des commentaires pour le Service d’authentification gouvernementale prévoyant la transmission à la personne responsable de la protection des renseignements personnels de toute plainte et de tout commentaire concernant la gestion des renseignements personnels, lesquels sont accessibles au personnel concerné. Les rôles et responsabilités sont définis pour tous les secteurs impliqués. MESS (Services Québec) mandaté pour la gestion des plaintes et des commentaires en lien avec l’utilisation du Service d’authentification gouvernementale. Registre des plaintes du MCN.



Québec