

RAPPORT ANNUEL 2024-2025 SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

SERVICE QUÉBÉCOIS D'IDENTITÉ NUMÉRIQUE

SERVICE D'AUTHENTIFICATION GOUVERNEMENTALE
EN VERTU DE LA *LOI FAVORISANT LA TRANSFORMATION
NUMÉRIQUE DE L'ADMINISTRATION PUBLIQUE*

ET

DE LA *LOI SUR LA GOUVERNANCE ET LA GESTION DES
RESSOURCES INFORMATIONNELLES DES ORGANISMES
PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT*

MINISTÈRE DE LA CYBERSÉCURITÉ
ET DU NUMÉRIQUE

Juin 2025

PRODUCTION

Direction générale du Service québécois d'identité numérique

Sous-ministériat adjoint au dirigeant de l'information et à la gouvernance

INFORMATION

Ministère de la Cybersécurité et du Numérique

900, place D'Youville, 3^e étage

Québec (Québec) G1R 3P7

418 644-1030

Courriel : information@mcn.gouv.qc.ca

Tous droits réservés pour tous pays. La reproduction, par quelque procédé que ce soit, la traduction ou la diffusion de ce document, même partielles, sont interdites. Cependant, la reproduction de ce document ou son utilisation à des fins personnelles, d'étude privée ou de recherche scientifique, mais non commerciales, sont permises à condition d'en mentionner la source.

© Gouvernement du Québec, 2025

Table des matières

Objectif	3
Contexte	3
Objectifs et motivation du projet et de la source officielle	4
Responsable du projet	5
Décisions du projet.....	6
Expérimentation	6
Changements significatifs.....	6
Renseignements personnels recueillis, utilisés ou communiqués....	6
Mesures mises en place pour assurer la protection des renseignements personnels.....	7
Responsable de la protection des renseignements personnels	8
Transmission et diffusion.....	8
Annexes	9
Annexe 1 – Vue d’ensemble de la circulation des renseignements personnels du Service d’authentification gouvernementale	9
Annexe 2 – Mesures mises en place pour assurer la protection des renseignements personnels.....	18

OBJECTIF

Le présent rapport répond aux obligations du ministère de la Cybersécurité et du Numérique (MCN) en matière de circulation des renseignements personnels dans le contexte du Programme Service québécois d'identité numérique (SQIN). Il vise plus spécifiquement les renseignements personnels recueillis, utilisés et communiqués par et pour le Service d'authentification gouvernementale, de même que ceux impliqués dans le cadre de la désignation du MCN en tant que source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale. Ce rapport 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) qui prévoit qu'un organisme public responsable de la gestion d'un projet en ressources informationnelles d'intérêt gouvernemental doit transmettre annuellement au ministre un rapport concernant l'utilisation et la communication de renseignements personnels nécessaires à la réalisation d'un projet en ressources informationnelles d'intérêt gouvernemental;
- 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) qui prévoit qu'un organisme public désigné comme source officielle de données numériques gouvernementales, tel que le MCN, doit produire un rapport annuel portant sur les renseignements personnels recueillis, utilisés ou communiqués et sur les mesures de protection mises en place pour assurer leur protection.

Le Service d'authentification gouvernementale a le statut de projet d'intérêt gouvernemental, en étant un projet qualifié du SQIN, et le MCN agit comme source officielle de données numériques gouvernementales pour les fins du Service d'authentification gouvernementale. Le MCN doit donc produire un rapport au ministre de la Cybersécurité et du Numérique, responsable de l'application de la LFTNAP et de la LGGRI, l'obligation d'en transmettre une copie à la Commission d'accès à l'information (CAI), d'en déposer une copie à l'Assemblée nationale et de veiller à sa diffusion. Ce rapport concerne les activités d'identification et d'authentification des citoyennes et des citoyens du Québec.

CONTEXTE

La mise en place du Programme SQIN vise à constituer une fondation innovante, propulsant le citoyen dans l'ère du numérique, lui procurant une identité numérique de confiance et lui simplifiant l'accès aux services gouvernementaux. Ce programme

comporte des projets en ressources informationnelles d'intérêt gouvernemental, dont le projet 1 « Accès bonifié aux prestations électroniques de services – Citoyens ».

Ce projet vise à mettre en place le Service d'authentification gouvernementale, y compris la création du Registre d'attributs d'identité gouvernemental (RAIG), pour permettre l'identification et l'authentification des personnes en vue de leur donner accès aux prestations électroniques de services (PES) gouvernementales. Il contribue également à la protection de l'intégrité et de la confidentialité des renseignements personnels détenus par l'État.

Le Service d'authentification gouvernementale a pour objectif d'offrir des services simplifiés, intégrés et de qualité qui s'appuient sur les technologies de l'information, y compris les technologies numériques, tout en assurant la pérennité du patrimoine numérique gouvernemental.

De plus, le gouvernement a désigné le MCN comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale (décret numéro 870-2022 du 25 mai 2022), déployé dans le cadre de la réalisation du projet 1 du Programme SQIN. Seules les données numériques gouvernementales requises pour la constitution et la tenue du RAIG sont communiquées au MCN par l'entremise du Fichier d'inscription des personnes assurées (FIPA) de la Régie de l'assurance maladie du Québec (RAMQ)¹. Le 18 décembre 2023, en vertu de l'article 12.21 de la LGGRI, le gestionnaire des données numériques gouvernementales a autorisé la mobilité de ces données numériques gouvernementales détenues par la RAMQ aux fins du Service d'authentification gouvernementale du 1^{er} janvier 2024 au 31 décembre 2026.

OBJECTIFS ET MOTIVATION DU PROJET ET DE LA SOURCE OFFICIELLE

Le projet 1 du Programme SQIN vise notamment à remplacer le service d'authentification clicSÉCUR pour permettre à un plus grand nombre de citoyens d'accéder plus facilement et de manière plus sécuritaire aux PES gouvernementales. La mise en place du Service d'authentification gouvernementale vise également l'uniformisation des façons de faire

¹ Vise 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.

des organismes publics (OP) en matière d'authentification des utilisateurs pour accéder à leurs services en ligne.

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 entraînera 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.

Les principaux objectifs du projet 1 sont les suivants :

- Améliorer la sécurité des renseignements personnels des citoyens;
- Simplifier le processus d'authentification gouvernementale et de vérification d'identité;
- Élargir le bassin de la clientèle potentielle aux PES gouvernementales;
- Implanter un service unifié d'authentification gouvernementale qui contribue à la confiance du public dans les solutions technologiques de l'administration publique;
- Fournir aux utilisateurs un Service d'authentification gouvernementale convivial, moderne, évolutif, extensible, sécuritaire et disponible.

RESPONSABLE DU PROJET

Le Secrétariat du Conseil du trésor a confié la responsabilité de la réalisation du Programme Service québécois d'identité numérique 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 1^{er} septembre 2020. La *Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions* (2021, chapitre 33) a été sanctionnée le 3 décembre 2021, ce qui abroge la *Loi sur Infrastructures technologiques Québec*. Le 1^{er} janvier 2022, le ministère de la Cybersécurité et du Numérique se voit confier les responsabilités qui étaient dévolues à Infrastructures technologiques Québec en vertu de sa loi constitutive.

DÉCISIONS DU PROJET

Par la prise du décret numéro 511-2020 du 13 mai 2020, le gouvernement a autorisé la phase d'exécution du projet 1 « Accès bonifié aux prestations électroniques de services – Entreprises et Citoyens » du Programme SQIN.

EXPÉRIMENTATION

Par la prise du décret numéro 1690-2022 du 26 octobre 2022, modifié par le décret numéro 766-2023 du 5 mai 2023, la RAMQ a été désignée pour communiquer au MCN les renseignements personnels qu'elle détient et qui sont nécessaires aux fins des expérimentations requises avant le déploiement du Service d'authentification gouvernementale, et ce, malgré l'article 63 de la *Loi sur l'assurance maladie* (chapitre A-29). Le chargement initial des renseignements personnels en provenance du FIPA de la RAMQ vers le RAIG du MCN s'est effectué le 11 novembre 2022.

En vertu de ces décrets, des expérimentations ont été effectuées avec le ministère de la Famille et la Société de l'assurance automobile du Québec afin de tester le fonctionnement et l'efficacité du Service d'authentification gouvernementale. Les expérimentations requises avant le déploiement du Service d'authentification gouvernementale ont été complétées le 31 décembre 2023.

CHANGEMENTS SIGNIFICATIFS

Par la prise du décret numéro 765-2023 du 3 mai 2023, le gouvernement a autorisé un changement significatif à la portée du projet 1 du Programme SQIN afin d'ajouter une plateforme de développement moderne spécifique à ce programme ainsi que des fonctionnalités nécessaires à la vérification de l'identité d'une personne dans un centre de services et au déploiement du Service d'authentification gouvernementale. Par la prise de ce décret, la phase d'exécution du projet a été prolongée jusqu'au 31 décembre 2023.

Par la prise du décret numéro 1848-2023 du 20 décembre 2023, le gouvernement a autorisé un changement significatif à la portée du projet 1 du Programme SQIN afin de retirer le bloc « Accès bonifié aux prestations électroniques de services – Entreprises » du projet et a autorisé la poursuite de la réalisation de la phase d'exécution du nouveau projet « Accès bonifié aux prestations électroniques de services – Citoyens ». Par la prise de ce décret, la phase d'exécution du projet a été prolongée jusqu'au 13 mai 2025.

Par la prise du décret numéro 1084-2024 du 10 juillet 2024, les OP visés à l'article 2 de la LGRI 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 pour une PES. Cette nouvelle exigence vise à faciliter les démarches 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.

Par l'adoption de l'indication d'application numéro IA-RI-2024-001-OP en date du 12 juillet 2024, le MCN a précisé certaines activités 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. Cette indication d'application appuie le décret numéro 870-2022 du 25 mai 2022.

RENSEIGNEMENTS PERSONNELS RECUEILLIS OU UTILISÉS

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 du ministère de la Cybersécurité et du Numérique » du présent rapport :

1. Une description des renseignements personnels recueillis par le MCN ou qui lui ont été communiqués ainsi que leur provenance;
2. Une description des objectifs pour lesquels les renseignements personnels sont recueillis et utilisés;
3. 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 atteste que l'ensemble des mesures appropriées ont été prises afin d'assurer la protection des renseignements personnels. Ces mesures 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 au 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. Une copie est également transmise au gestionnaire des données numériques gouvernementales et, conformément à l'article 12.18 de la même loi, le rapport est diffusé sur le site Internet du MCN.

ANNEXES

Annexe 1 – Vue d’ensemble de la circulation des renseignements personnels du Service d’authentification gouvernementale

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	Provenance	Description des finalités	Moyen d’interaction et modalité
Renseignements personnels prévus au décret : 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	RAMQ	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 permettre d’avoir accès aux PES gouvernementales ² . 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).	Chargement initial des renseignements personnels en provenance du FIPA de la RAMQ vers le RAIG du MCN ³ et transmission d’une mise à jour des renseignements personnels ██████████ dans un canal sécurisé (aucune transmission inverse possible). <i>Note : Le NAM et le NAS sont des renseignements personnels sensibles qui font l’objet d’une protection équivalente à celle contenue dans les règles particulières de protection mises en place dans le cadre des expérimentations⁴.</i>

² Conformément au décret numéro 1690-2022 du 26 octobre 2022 modifié par le décret numéro 766-2023 du 3 mai 2023.

³ Ibid.

⁴ Ibid. Règles particulières de protection du NAS et du NAM dans le cadre des expérimentations requises avant le déploiement du SAG du projet d’intérêt gouvernemental, Programme SQIN.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	Provenance	Description des finalités	Moyen d'interaction et modalité
Numéro d'assurance maladie (NAM) Numéro d'assurance sociale (NAS) Identifiant sectoriel de la RAMQ			
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	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 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 (détermination d'une période de validité de l'adresse de résidence active).	Transmission d'une mise à jour des renseignements personnels 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 Mot de passe Code de sécurité	Utilisateurs du Service d'authentification gouvernementale	Création, modification et accès à un 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 à un compte au Service d'authentification gouvernementale, et aux fins d'authentification des personnes pour leur permettre d'avoir accès au Service d'authentification gouvernementale. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : Adresse courriel : renseignement personnel utilisé aux fins de correspondance. Code de sécurité [REDACTED] deuxième facteur d'authentification [REDACTED]. [REDACTED] [REDACTED] [REDACTED]	Interface d'échanges informatisé du Service d'authentification gouvernementale. Transactions informatiques [REDACTED] [REDACTED] Génération automatique d'un code de sécurité. [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	Utilisateurs du 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 pour leur permettre d'avoir accès aux PES gouvernementales. 	Interface d'échanges automatisé du Service d'authentification gouvernementale. Transactions informatiques sécurisées

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]	Utilisateurs du Service d'authentification gouvernementale MCN [REDACTED]	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 pour leur permettre d'avoir accès aux PES gouvernementales. Au surplus des finalités mentionnées 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 : renseignement personnel recueilli et utilisé aux fins de correspondance. [REDACTED] [REDACTED]	Interface d'échanges automatisé du Service d'authentification gouvernementale. Transactions informatiques sécurisées [REDACTED]. Génération d'un secret d'identification par la poste [REDACTED]. [REDACTED] Génération automatique d'une lettre.

[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 Adresse courriel Code de sécurité Signature Types des pièces d'identité fournies, dont une avec photo	Utilisateurs du 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 gouvernementales⁶. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : Signature : renseignement personnel recueilli aux fins de manifestation d'un consentement exprès à l'utilisation et à la communication des renseignements personnels. Code de sécurité [REDACTED] deuxième facteur d'authentification [REDACTED]. Type des pièces d'identité fournies : renseignement personnel recueilli aux fins de vérification à postériori.	Collaboration avec un OP partenaire aux fins du processus d'identification [REDACTED] des utilisateurs dans un point de service autorisé. Entente entre l'OP partenaire et le MCN. Formulaire papier de consentement. Échanges dans un point de service. Interface d'échanges automatisé [REDACTED]. Transactions informatiques sécurisées [REDACTED].

⁶ En vertu du décret numéro 765-2023 du 3 mai 2023.

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	Provenance	Description des finalités	Moyen d'interaction et modalité
Nom DDN NAM Adresse courriel Adresse de résidence Renseignements en lien avec l'utilisation d'un compte au Service d'authentification gouvernementale Numéro de téléphone	Utilisateurs du Service d'authentification gouvernementale Ministère de l'Emploi et de la Solidarité sociale (Services Québec)	Demande d'intervention au compte Renseignements personnels communiqués au MCN et utilisés, sur la base du consentement, pour l'identification des utilisateurs 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 des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : Adresse courriel : renseignement personnel utilisé aux fins de correspondance. Spécifiquement pour les renseignements personnels suivants : Numéro de téléphone : renseignement personnel utilisé aux fins de correspondance.	Collaboration avec un OP partenaire pour assurer le service à la clientèle de première ligne, incluant les demandes d'intervention au compte, et la gestion des plaintes et commentaires. Communication téléphonique. Notifications transmises par courriel. Formulaire électronique de demande d'intervention au compte. Partage sécurisé de document. Interface d'échanges automatisé [REDACTED]. Transactions informatiques sécurisées [REDACTED]. Formulaire Web de plainte ou de commentaire. Transmission [REDACTED] sécurisé de la plainte ou du commentaire au responsable des plaintes et des commentaires.
		Plainte ou commentaire Seuls les renseignements fournis parmi les suivants sont communiqués au MCN et utilisés, sur la base du consentement, aux fins de correspondance pour traiter une plainte ou un commentaire : nom, adresse courriel et numéro de téléphone.	

Renseignements personnels recueillis, utilisés ou communiqués au MCN			
Description des renseignements personnels	Provenance	Description des finalités	Moyen d'interaction et modalité
Identifiants [REDACTED] [REDACTED] [REDACTED] Adresse IP Ville et pays	Utilisateurs du 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]. Au surplus des finalités mentionnées ci-dessus et spécifiquement pour les renseignements personnels suivants : Ville et pays : renseignements personnels inférés à partir de l'adresse IP.	[REDACTED] Transactions informatiques sécurisées [REDACTED] [REDACTED]
Identifiants [REDACTED] [REDACTED] [REDACTED]	MCN [REDACTED]	Statistiques Renseignements personnels utilisés aux fins de production de statistiques pour évaluer la performance et 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
Identifiant [REDACTED] [REDACTED] Adresse courriel ou nom d'utilisateur Langue d'affichage : FR (pour français) ou EN (pour anglais)	Utilisateurs du Service d'authentification gouvernementale MCN [REDACTED]	Témoins de connexion Renseignements personnels utilisés afin d'assurer le bon fonctionnement du site Web du Service d'authentification gouvernementale, mais aussi d'améliorer et de personnaliser l'expérience utilisateur.	Transactions informatiques sécurisées [REDACTED] [REDACTED].

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 projet	Règles encadrant les renseignements personnels détenus aux fins du projet adopté et accessibles au personnel du MCN concerné. Règles de gouvernance encadrant les renseignements personnels détenus aux fins du projet transmises à la Commission d'accès à l'information pour information.
Formation et sensibilisation en matière de renseignements personnels	Activités de formation et de sensibilisation offertes aux employés concernés de la direction générale responsable du projet. Processus d'accueil et d'intégration pour tout nouvel employé de la direction générale responsable du projet. Registre des activités de sensibilisation et de formation en matière de protection des renseignements personnels, accessible au personnel concerné. Révision en continu du plan de formation et de sensibilisation.
Ressources dédiées à la protection des renseignements personnels	Soutien-conseil en continu pour le développement et l'exploitation du Service d'authentification gouvernementale dans le respect des obligations tout au long du cycle de vie des renseignements personnels.
Ententes contractuelles avec les tiers sur l'encadrement, notamment la communication de renseignements personnels à l'extérieur du Québec	Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers, accessible au personnel concerné. Lignes directrices du Courtier en infonuagique qui favorise 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 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

Énoncé	Mesure mise en place
	██████████ 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 SI basé sur le standard SSAE 16/SOC 2 Type II, attestations de destruction) pour démontrer leur conformité. Travaux en cours auprès des OP partenaires pour la mise en œuvre des activités d'audit externe. Registre en application de l'article 67.3 de la <i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i> (entente de collecte en collaboration avec un autre organisme et communication sans consentement), accessible au personnel concerné.
Rapports en application des lois applicables	Rapport d'EFVP transmis à la CAI pour information, accessible au personnel concerné.
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). Consultation menée par Votepour.ca sur la fracture numérique des personnes citoyennes (janvier 2024). Analyse et élaboration d'un plan d'action (mai 2024). Planification des travaux pour la mise en œuvre d'un plan d'action. 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).

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.

Énoncé	Mesure mise en place
	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 organismes publics 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.

Limitation de la collecte

Énoncé	Mesure mise en place
Légitimité à collecter les renseignements personnels aux fins déterminées	Projet « Accès bonifié aux prestations électroniques de services – Entreprises et Citoyens » du Programme SQIN désigné par décret comme projet en ressources informationnelles d'intérêt gouvernemental. Désignation du MCN, par décret, pour agir comme source officielle de données numériques gouvernementales aux fins du Service d'authentification gouvernementale.
Limitation de la collecte de renseignements personnels à ce qui est nécessaire aux fins déterminées	Évaluation de la nécessité de la collecte des renseignements personnels par rapport aux objectifs du projet et à la solution proposée, et ce, avant la prise du décret numéro 870-2022 du 25 mai 2022. 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. Ce processus comprend notamment la constitution et la tenue du RAIG, la création, la modification et l'accès

Énoncé	Mesure mise en place
	à un compte au Service d'authentification gouvernementale ainsi que le processus d'identification en ligne et en personne. Propositions faites à l'utilisateur afin de limiter la collecte de ses renseignements personnels (Politique de confidentialité du Service d'authentification gouvernementale). Champs à remplissage obligatoires prédéterminés dans l'interface d'échanges automatisé du Service d'authentification gouvernementale 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 <u>renseignements personnels sensibles</u> aux fins déterminées	Analyse de plusieurs combinaisons de renseignements personnels pour la réalisation du processus d'identification (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 piratage psychologique. 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'un citoyen. Combinaison du NAS et du NAM permettant de garantir la qualité des données en assurant en amont la fiabilité lors de l'identification 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. Accompagnement des équipes spécialisées dans toutes les phases du projet afin d'assurer l'intégration des mesures relatives à la protection de la vie privée.
Protection de la vie privée par défaut	Solution administrée selon les règles et les protocoles établis pour assurer le plus haut niveau de confidentialité sans intervention des utilisateurs. Paramétrage des fonctionnalités assurant le plus haut niveau de confidentialité sans intervention des utilisateurs. Évaluation en continu des témoins de connexion utilisés aux fins du Service d'authentification gouvernementale. Informations fournies aux utilisateurs quant à l'utilisation des témoins de connexion, notamment le témoin de profilage (fenêtre informative et Politique de confidentialité du Service d'authentification gouvernementale). Informations fournies à l'utilisateur quant aux moyens pour activer la fonction de localisation ou la refuser (fenêtre informative et Politique de confidentialité du Service d'authentification gouvernementale).

Consentement

Énoncé	Mesure mise en place
Consentement valide	Accompagnement des équipes spécialisées dans toutes les phases du projet afin d'assurer le respect des critères de validité du consentement. Forme du consentement et méthode d'obtention appropriées à la sensibilité des renseignements personnels impliqués et adaptés aux personnes visées, au contexte et au type d'interface. Informations requises fournies à l'utilisateur au moment de la demande de consentement spécifiant notamment les finalités de l'utilisation ou de la communication concernée. Informations fournies à l'utilisateur concernant les conséquences d'un refus ou, le cas échéant, d'un retrait de son consentement suivant une demande facultative.

Énoncé	Mesure mise en place
Exceptions au consentement	Obtention du consentement pour toute utilisation et communication de renseignements personnels aux fins déterminées, sauf exception comme pour la comparaison de données pendant la période requise de transition.
Documentation de l'obtention du consentement	Journalisation des événements liés au consentement. Formulaire de consentement papier.
Retrait du consentement	Informations fournies à l'utilisateur concernant son droit de retrait du consentement (Politique de confidentialité du Service d'authentification gouvernementale).

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

Énoncé	Mesure mise en place
Utilisation et communication aux seules fins déterminées	Politique de confidentialité et de protection des renseignements personnels du ministère de la Cybersécurité et du Numérique agissant à titre de source officielle de données numériques gouvernementales, accessible au personnel concerné. 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, accessible au personnel concerné. 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 à la confidentialité, à la disponibilité ou à l'intégrité. Analyse par les équipes spécialisées des demandes d'utilisation et de communication de renseignements personnels détenus aux fins du Service d'authentification gouvernementale à des fins compatibles (primaires et secondaires) pour réaliser certaines activités en accord avec le décret. 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.

Énoncé	Mesure mise en place
	Limitation de la communication des renseignements personnels nécessaires au suivi d'une demande d'intervention à un compte au Service d'authentification gouvernementale; seul le numéro de la demande est communiqué à l'utilisateur. Registre en application de l'article 67.3 de la <i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i> (utilisation à une autre fin), accessible au personnel concerné. 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.
Conservation des renseignements personnels pour la réalisation des fins déterminées	Politique de confidentialité et de protection des renseignements personnels du ministère de la Cybersécurité et du Numérique agissant à titre de source officielle de données numériques gouvernementales, accessible au personnel concerné. 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, accessible au personnel concerné. Règle de conservation pour les renseignements personnels contenus dans le RAIG, établie par le MCN et approuvée par la Bibliothèque et Archives nationales du Québec (BANQ). Toute modification apportée à un renseignement personnel au FIPA de la RAMQ entraîne une modification du renseignement personnel concerné au RAIG (aucune conservation d'historique des renseignements personnels modifiés). Programme d'élaboration du Plan de destruction de renseignements personnels détenus aux fins du Service d'authentification gouvernementale. Formulaire de consentement papier conservé le temps nécessaire pour respecter les obligations légales de conservation décrites dans la <i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i>. 

Exactitude

Énoncé	Mesure mise en place
Assurance de la qualité des renseignements personnels détenus aux fins du Service d'authentification gouvernementale	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. Informations fournies à l'utilisateur au regard de sa responsabilité concernant la mise à jour de ses renseignements personnels (Politique de confidentialité du Service d'authentification gouvernementale). Transmission d'une mise 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. Champs à remplissage Service d'authentification gouvernementale prédéfinis pour la saisie des renseignements personnels dans l'interface d'échanges automatisé du Service d'authentification gouvernementale. Règles d'affaires mises en application pour valider la qualité des données, comprenant des renseignements personnels [REDACTED]. Règles d'affaires mises en application pour la gestion des adresses de résidence en vue de la transmission de correspondance. Mise à jour de l'adresse courriel et du mot de passe par l'entremise de la gestion de compte en ligne. Mise à jour de l'adresse courriel par l'entremise d'une demande téléphonique d'intervention au compte. Journalisation des événements liés à certaines mises à jour.

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 déployant d'une infrastructure technologique sécuritaire.

Énoncé	Mesure mise en place
	Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques [REDACTED]. Cadre normatif en matière de renseignements personnels, de SI et des conflits d'intérêts. Plusieurs types de mesures⁷ 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 de cibler 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, la mise en place de mots de passe ou de mécanismes d'authentification à facteurs multiples; • des mesures organisationnelles, comme l'adoption et l'application de règles en matière de SI et de protection des renseignements personnels, plan de reprise en cas de sinistre. Notifications transmises automatiquement par courriel aux utilisateurs pour les informer de la survenance d'événements 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.
Gestion des accès	Processus de révision de l'identité et des droits d'accès, accessible au personnel concerné.

⁷ La liste complète des mesures applicables au SAG et au RAIG n'est pas accessible pour des raisons de sécurité.

Énoncé	Mesure mise en place
	Renseignements personnels accessibles aux personnes qui détiennent les autorisations requises lorsque cela est nécessaire à l'exécution de leurs tâches. Rôles et responsabilités des intervenants établis dans le Service d'authentification gouvernementale (profils d'accès fondés sur les tâches, mode consultation).  Droit d'accès aux renseignements personnels sensibles octroyés de façon ponctuelle et temporaire pour répondre à une demande précise et assortie d'un délai prédéfini. Mécanismes de contrôle et de surveillance des droits d'accès afin de détecter les abus de droit, le cas échéant : • Journalisation de tout accès aux renseignements personnels; • Analyse automatisée et périodique des journaux afin de déceler les anomalies ou les irrégularités; • Alerte déclenchée pour tout accès aux renseignements personnels contenus dans le RAIG et vérification visant à confirmer le droit d'accès; • Registre des membres du personnel ayant un accès physique ou informatique aux renseignements personnels détenus aux fins du Service d'authentification gouvernementale, accessible au personnel autorisé. Inventaire des catégories de personnes qui ont accès aux renseignements personnels, accessible au personnel concerné.
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. Processus de gestion des incidents de SI, qui relève du Centre organisationnel de cyberdéfense, prévoyant l'implication du responsable

Énoncé	Mesure mise en place
	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 CAI 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.

