Ministère
de la Cybersécurité
et du Numérique
Québec

Direction du Secrétariat général adjoint et de l'accès à l'information

PAR COURRIEL

Québec, le 5 septembre 2025

[redacted]

N/Réf. : DA2526-20

Objet : Votre demande en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)

[redacted],

Par la présente, nous donnons suite à votre demande reçue le 6 août 2025 visant à obtenir :

> « ... copie de toutes évaluations des facteurs relatifs à la vie privée réalisées depuis le 22 septembre 2023 jusqu'à ce jour ».

En réponse à votre demande, nous vous transmettons des documents détenus par le ministère de la Cybersécurité et du Numérique (MCN). Toutefois, certaines informations sont caviardées en vertu des articles 22, 29, 37, 53, 54 et 59 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, ci-après nommée « Loi sur l'accès »)*.

Également, certains documents détenus par le MCN ne peuvent vous être transmis conformément à l'article 9 de la *Loi sur l'accès*.

Par ailleurs et en application à l'article 13 de la *Loi sur l'accès*, vous pourrez consulter l'évaluation des facteurs relatifs à la vie privée du *Service d'authentification gouvernementale* (SAG) qui fera l'objet d'une diffusion sur Québec.ca au cours des prochains mois.

Conformément à l'article 51 de la *Loi sur l'accès,* nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information dans les 30 jours suivant la date de la présente.

...2

900, place D'Youville
Québec (Québec) G1R 3P7
Téléphone : 418 644-1500
acces@mcn.gouv.qc.ca

À cet effet, vous trouverez, ci-joints, le texte des articles précités ainsi qu'une note explicative concernant l'exercice de ce recours.

Je vous prie d'agréer, [redacted], nos salutations distinguées.

La responsable de l'accès aux documents,

Original signé

Isabelle Goulet

Ministère
de la Cybersécurité
et du Numérique
Québec

SOLUTION GOUVERNEMENTALE DE GESTION DES APPRENTISSAGES (SGGA)

Rapport d'évaluation des facteurs relatifs à la vie privée

Ministère de la Cybersécurité et du Numérique

Date du document : 1er octobre 2024

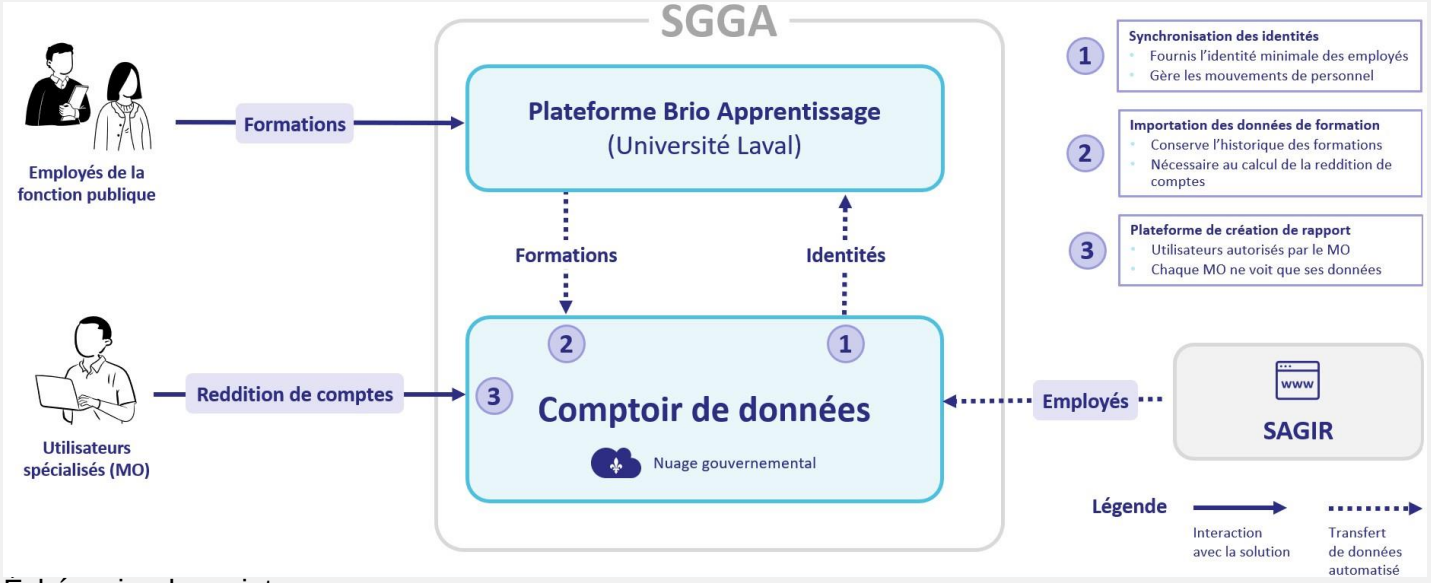
Dernière révision : *Cliquez ou appuyez ici pour entrer une date.*

TABLE DES MATIÈRES

RÉSUMÉ DE L'ÉVALUATION

IDENTIFICATION DU RESPONSABLE DE L'ÉVALUATION	
Nom du responsable	Natacha Beaumont
Titre et/ou responsabilité	Directrice du projet SGGA et Chef du Service des solutions d'affaires gouvernementales
Direction et/ou service	Direction des solutions d'affaires gouvernementales (SMATNG)
Coordonnées	Ministère de la Cybersécurité et du Numérique SMATNG, DGSEAOASG, DSAG, SCSAG 800 chemin Sainte-Foy, 7e étage, Québec (Québec) G1S 2L2

AUTRES PERSONNES IMPLIQUÉES DANS L'ÉVALUATION		
Nom	**Titre**	**Organisation**
Karima El Ouazzani	Responsable de produit Comptoir de données	MCN-SMATNG-DSAG-SSAG
Tariq Mahjoubi	Analyste d'affaires	MCN-SMATNG-DSAG-SSAG
Maxime Arseneau	Conseiller en gestion du changement	MCN-SMATNG-DSAG-SSAG
Brice Boulangeot	Architecte intégrateur	MCN-SMATNG-DSAG-SSAG
Claire Chevalier	Coordinatrice	MCN-SMATNG-DSAG-SSAG
Diane Laurent	Conseillère experte en protection des renseignements personnels	MCN-SMAPIG-DGDNGO-DGOPVP
Youri Tacoun	Conseiller en gestion intégrée des risques	MCN – DGBSMSG – DSGAAI
Chantal Dumond	Conseillère APPI	APPI

<table>
<tr><th colspan="3">DESCRIPTION DU PROJET</th></tr>
<tr><td>Description sommaire</td><td colspan="2">La solution gouvernementale de gestion des apprentissages (SGGA) est un environnement numérique d’apprentissage et de développement des compétences pour les membres du personnel de la fonction publique.
Elle est composée de la plateforme Brio Apprentissage (développée par l’Université Laval) et d’un Comptoir de données (développé par le MCN) pour la reddition de comptes – formation et développement.
Le projet est porté par les acteurs suivants :
- Secrétariat du Conseil du trésor (SCT), gouvernance de la solution et promoteur affaires
- Ministère de la Cybersécurité et du Numérique (MCN), gestion du changement, responsable de la solution, comptoir des données,
- Université Laval, accompagnement dans le déploiement de Brio Apprentissage.</td></tr>
<tr><td>Date de début du projet</td><td colspan="2">Été 2022</td></tr>
<tr><td>Durée prévue du projet (ou autres informations temporelles pertinentes)</td><td colspan="2">Voir
 

Échéancier du projet</td></tr>
<tr><td colspan="2">Le projet implique des renseignements personnels.</td><td>Oui ☒ / Non ☐</td></tr>
</table>

RÉSUMÉ DE L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

		Oui	Non
Le projet implique la **réalisation obligatoire d'une EFVP** en vertu d'une loi.		☒	☐
Si **oui**, indiquer la loi concernée ainsi que le ou les articles applicables	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LADOPPRP) et Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI)		
Statut de ce rapport	☒ Nouveau	☐ Modification d'un rapport existant – préciser :	

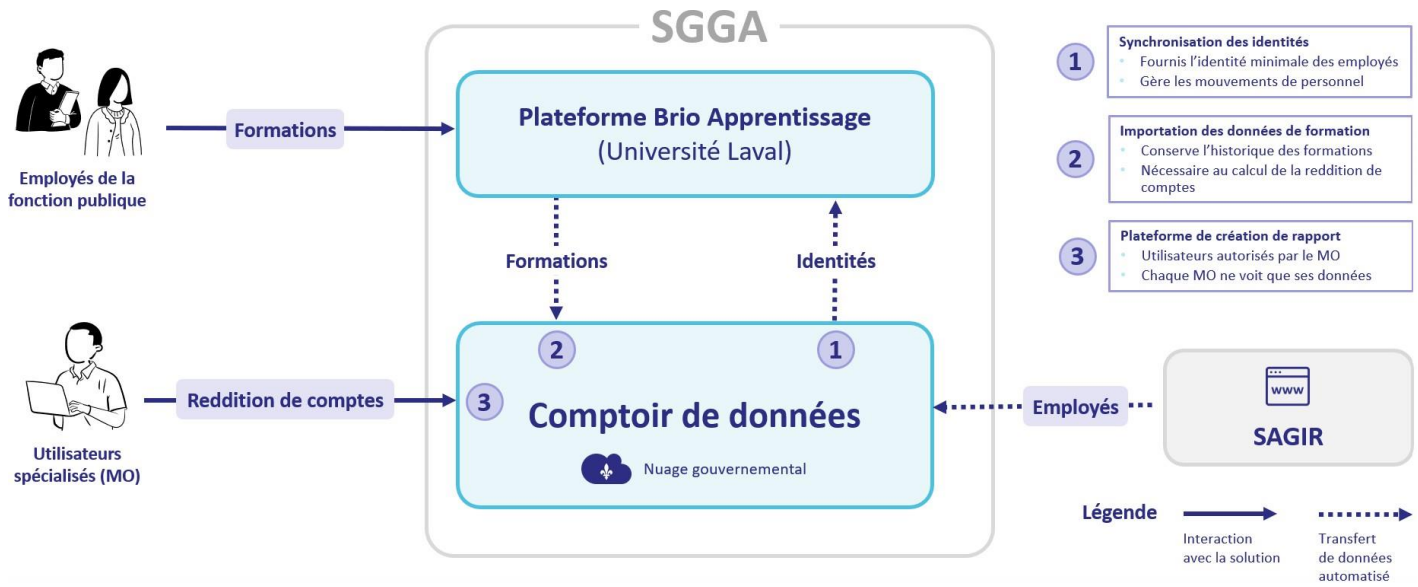
	Oui	Non
Dans le cadre de cette évaluation, le **projet, ses objectifs et l'objet de l'EFVP** ont été **définis.**	☒ cf. section 1	☐
L'**inventaire des renseignements personnels** et leur **parcours** ont été réalisés.	☒ cf. section 2	☐
L'ampleur de **l'évaluation est proportionnelle** à la **sensibilité** des renseignements personnels impliqués dans le projet, à la **finalité** de leur utilisation, à leur **quantité** à leur **répartition,** à leur **support.**	☒ cf. section 2	☐
Les **acteurs pertinents** ont été impliqués dans l'évaluation et les **rôles et les responsabilités** de chacun ont été précisés.	☒ cf. section 3	☐
L'organisation s'est assurée de **respecter les obligations** et les **principes** de **protection de renseignements personnels.**	☒ cf. section 4	☐
L'organisation a **identifié les risques** à la vie privée engendrée par le projet, ciblé leurs **causes** et évalué leur **probabilité** et leurs **conséquences potentielles.**	☒ cf. section 5	☐
L'organisation a **prévu des stratégies** pour éviter ou réduire ces risques efficacement.	☒ cf. section 5	☐
Des **mécanismes de suivi de l'évaluation** ont été mis en place.	☒ cf. section 6	☐

1. DESCRIPTION DU PROJET ET DE L'OBJET DE L'EFVP

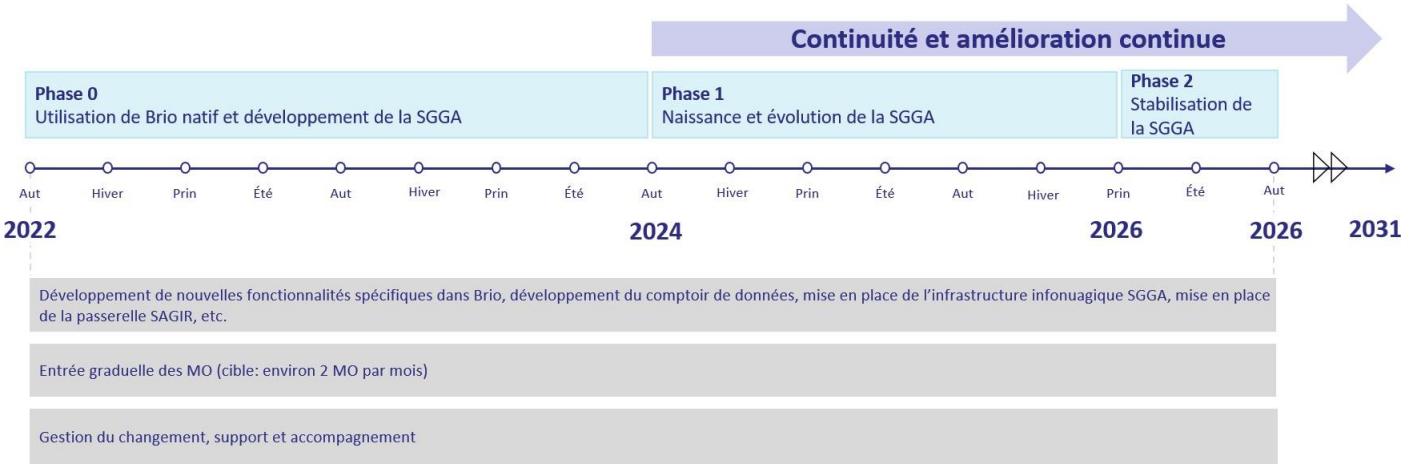
Présentation des grandes lignes du projet

La solution gouvernementale de gestion des apprentissages (SGGA) est un environnement numérique d'apprentissage et de développement des compétences pour les membres du personnel de la fonction publique ; composée de :

- La plateforme Brio Apprentissage, et
- d'un Comptoir de données.



Échéancier du projet



Énoncé et justification des objectifs motivant le projet

Objectifs de la solution :

- Offrir une solution de gestion des apprentissages uniforme et centrale pour l'ensemble des organisations de la fonction publique.
- Améliorer et simplifier la reddition de comptes afin de répondre aux exigences légales et normatives en matière de développement des compétences.
    - Loi favorisant le développement et la reconnaissance des compétences de la main-d'œuvre (1%).
    - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (publication des dépenses de formation des MO).
    - Loi sur l'administration publique (reddition de comptes) sur l'obligation de préparation d'un rapport annuel de gestion.
- Uniformiser et conserver l'historique des dossiers des apprenants tout au long de leur carrière au sein du gouvernement permettant de soutenir leur parcours de développement.

Un projet en adéquation avec les stratégies et les plans d'action gouvernementaux, qui s'appuie sur les stratégies de gestion des ressources humaines depuis 2018 (2018-2023, 2019-2023, 2023-2028) :

- Répondre aux enjeux actuels et futurs du marché de l'emploi et mettre en œuvre une culture organisationnelle renouvelée axée sur l'innovation et la performance.
- Le numérique pour une administration publique innovante, efficiente et transparente.
- La Stratégie de gestion des ressources humaines de la fonction publique 2023-2028 met l'accent sur des organisations apprenantes et des parcours professionnels épanouissants dans l'axe 2.
  Axe 2 – Culture d'organisation apprenante : l'ensemble de l'effectif doit pouvoir saisir toutes les occasions de développement.
  Objectif 3 : Mise en œuvre d'un environnement d'apprentissage de la fonction publique.

Démonstration que le projet est proportionné aux objectifs et aux risques d'atteinte à la vie privée

[Note] Notion de nécessité et proportionnalité ; source : Commission d'Accès à l'Information - Ministères et organismes publics : Collecte de renseignements personnels

L'évaluation de la nécessité de collecter des renseignements personnels doit prédominer en toute circonstance. Elle permet de minimiser l'atteinte à la vie privée des personnes concernées. Elle est réalisée avant la collecte des renseignements personnels par les organismes publics. […] [Elle] prévaut en toute circonstance […].

La nécessité va au-delà de la simple utilité. Pour un organisme public, elle s'évalue par rapport à la finalité de la collecte et à sa proportionnalité. Ainsi, une collecte sera nécessaire si ces conditions sont toutes réunies : l'objectif poursuivi est légitime, important et réel; l'atteinte à la vie privée est proportionnelle à cet objectif, ce qui signifie plus précisément que : la collecte des renseignements est rationnellement liée aux objectifs.

L'atteinte au droit à la vie privée est minimisée. Autrement dit, il n'existe pas d'autres moyens d'atteindre les mêmes objectifs d'une façon qui porterait moins atteinte à la vie privée.

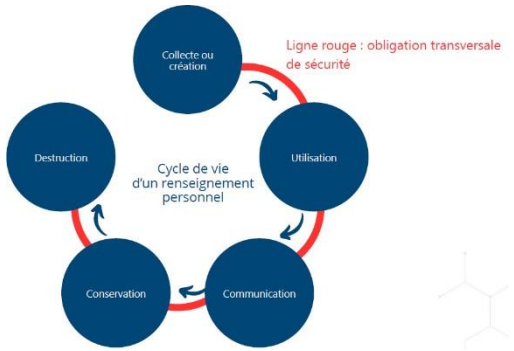
La collecte, l'utilisation ou la communication du renseignement est nettement plus utile à l'organisme que préjudiciable à la personne concernée.

Si la nécessité n'est pas établie, le droit à la vie privée des personnes doit primer. La collecte ne peut donc pas être effectuée.

[redacted]

La démarche proposée par l'accompagnement de l'AAPI et de l'équipe PRP du MCN est fondée sur l'analyse du cycle de vie de la protection des renseignements personnels. Ce cycle de vie est découpé en cinq (5) :

- Collecte ou création du renseignement personnel : nécessité (objectifs légitime, important et réel) et proportionnalité (sensibilité, répartition, supporté, quantité, finalité).
- Utilisation : fins initiales ou secondaires, consentement distinct.
- Communication : à la personne, à un tiers, avec ou sans consentement.
- Conservation : repérage, accessibilité, sécurité.
- Destruction ou anonymisation.



[redacted]

Détermination de l’objet de l’évaluation

La présente évaluation s’inscrit dans le cadre de la Loi sur l’accès, article 63.5 introduisant le principe de la protection de la vie privée dès la conception.

L’article 63.5 précise qu’un organisme public doit procéder à une EFVP de tout projet d’acquisition, développement ou refonte d’un système d’information ou d’une prestation électronique de services qui impliquerait la collecte, l’utilisation, la communication, la conservation ou la destruction de renseignements personnels.

Pour la Commission d’Accès à l’Information (CAI)[1], l’évaluation des facteurs de la vie privée est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

L’objet de l’évaluation est :

- La détermination des risques d’atteintes à la vie privée engendrés par le projet SGGA,
- L’évaluation de la conséquence de ces risques.
- La mise en place de stratégies pour les éviter ou les réduire.

[1] Guide d’accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée. À consulter également : Commissariat à la protection de la vie privée du Canada (guide)

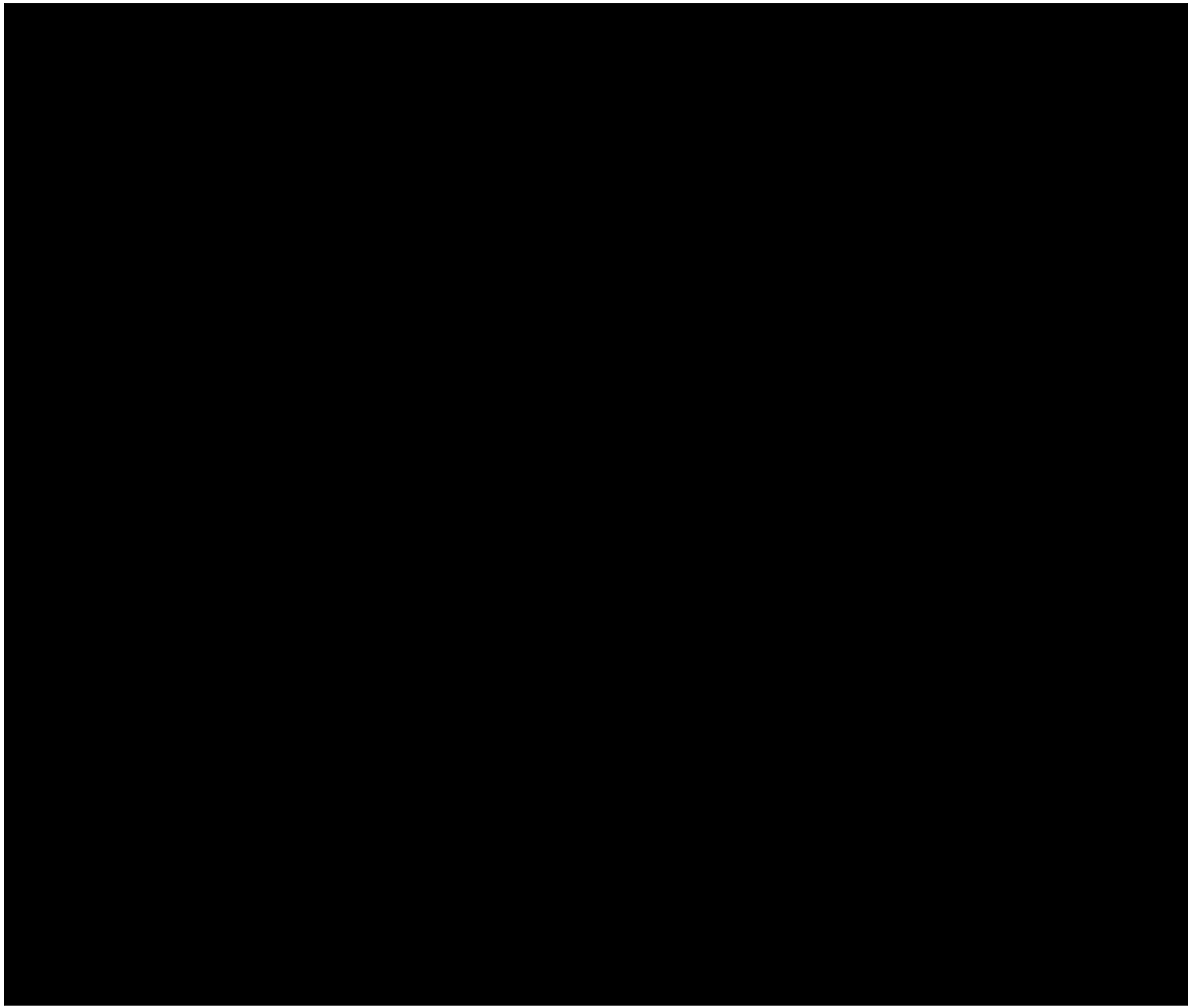
3. RENSEIGNEMENTS PERSONNELS IMPLIQUÉS ET AMPLEUR DE L'ÉVALUATION

Inventaire des renseignements personnels impliqués

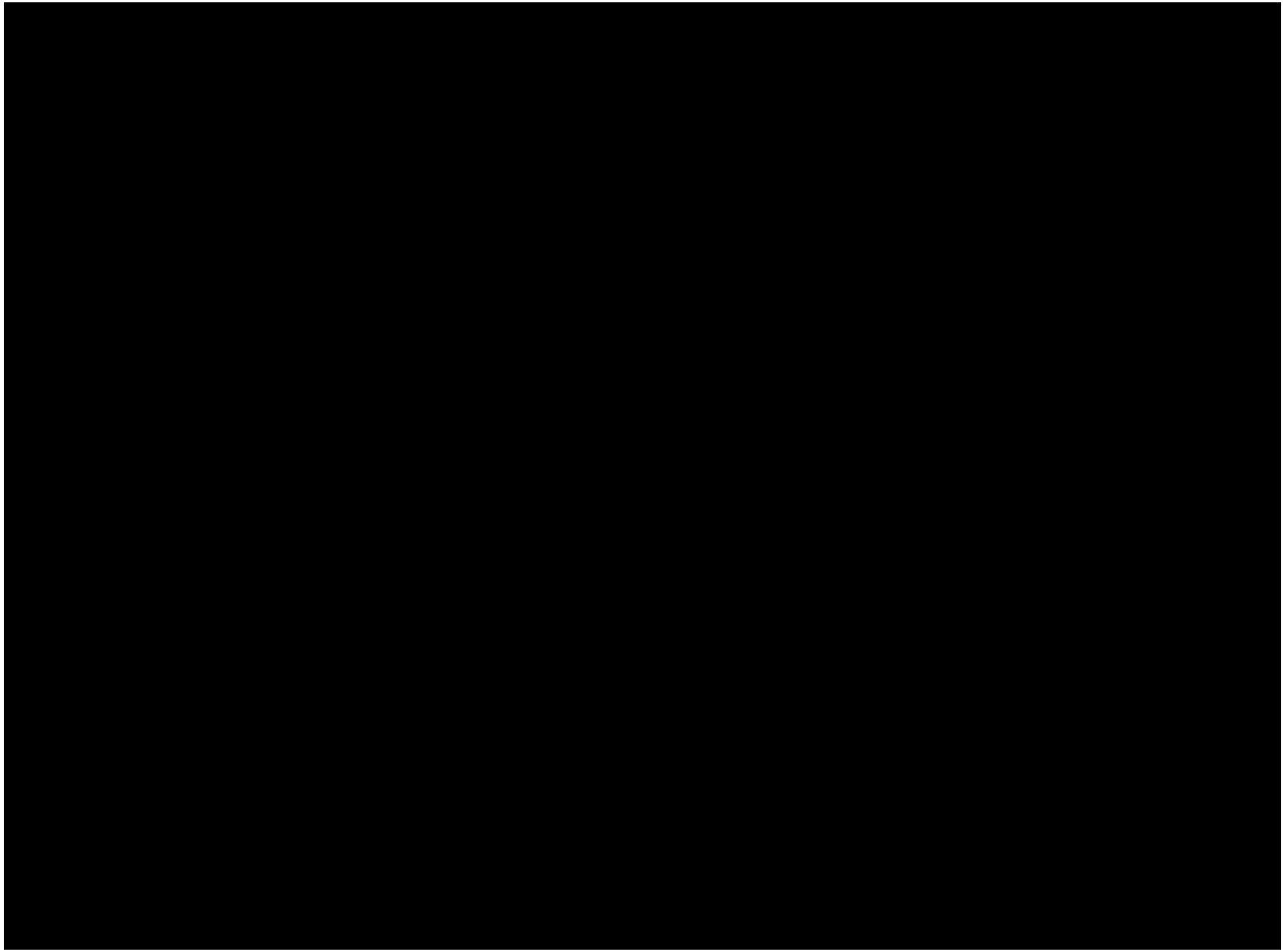
- Voir section : 1. Description du projet et de l'objet de l'EFVP

CATÉGORIES DE PERSONNES DONT LES RENSEIGNEMENTS SONT VISES

Catégorie	Détails
☒ Clientèle	Membre du personnel de la fonction publique, des ministères et organismes utilisant la SGGA.
☒ Personnel de l'organisation	Membre du personnel de la fonction publique et de l'organisation MCN utilisant la SGGA.
☐ Autre(s)	*Préciser*
Nombre approximatif de personnes concernées :	Ensemble de l'effectif régulier de la fonction publique québécoise, dans la limite de 70 000 personnes.



Parcours des renseignements personnels



MOYENS UTILISÉS POUR TRAITER LES RENSEIGNEMENTS PERSONNELS

Phase du cycle de vie
Moyens pour recueillir les renseignements

Phase du cycle de vie
Moyens pour utiliser les renseignements
Moyens pour communiquer les renseignements
Moyens pour conserver les renseignements **(inclure des précisions sur le lieu de stockage)**
Moyens pour détruire les renseignements ou, s'il y a lieu, pour les anonymiser

[redacted]

[redacted]

CATÉGORIES DE PERSONNES QUI AURONT ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Rôle	Nombre de personnes exerçant ce rôle	Type d'accès*	[redacted]	Explications sur la nécessité pour ces personnes d'avoir accès aux renseignements
Administrateur ou Pilote MO	Responsabilité interne de chaque MO –	Pilotage		Administrer/piloter la solution pour le compte du MO
	Cible : une (1) à deux (2) personnes par MO			
Responsable de la reddition des comptes	Responsabilité interne de chaque MO – cible : cinq (5) à dix (10) personnes par MO	Générer les rapports		Exporter des données pour suivi et reddition de compte
Responsable de la reddition des comptes avec droit de saisie	Responsabilité interne de chaque MO – cible : deux (2) à cinq (5) personnes par MO	Écriture		*En cours de définition,* saisir certaines dépenses/coûts, informations contractuelles dans le cadre de la gestion des formations.

*La définition des types d'accès est en cours d'analyse.

4. CONFORMITÉ AUX OBLIGATIONS ET AUX PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Obligations applicables

Loi / Règlement / Norme / Autre	Articles / dispositions applicables, s'il y a lieu	Mesures prises
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LADOPPRP)	Article 63.5	Pour plus d'informations, voir les sections suivantes : 5. Identification des risques et des stratégies pour les atténuer et 6. Plan d'action
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI)	Articles 12.15 à 12.19	
Loi favorisant le développement et la reconnaissance des compétences de la main-d'œuvre (1%)	Articles 3 et suivants	

5. IDENTIFICATION DES RISQUES ET DES STRATÉGIES POUR LES ATTÉNUER

Risques à la collecte

#	[redacted]	Risques potentiels	[redacted]
1		Collecte excessive de renseignements	
2		Collecte sans consentement	
3		Manque d'information fourni aux individus lors de la collecte	
4		Non-conformité : Difficulté à exercer ses droits d'accès et de rectification	

Risques à l’utilisation

PRÉCISIONS

Sans objet

Risques à la communication

PRÉCISIONS

Sans objet

Risques à la conservation, à la destruction et/ou à l’anonymisation

#	[redacted]	Risques potentiels	[redacted]
5		Conservation au-delà de ce qui est nécessaire (risque)	
6		Conservation au-delà de ce qui est nécessaire (risque)	

	[redacted]		
7	[redacted]	Réidentification de renseignements préalablement dépersonnalisés	[redacted]

PRÉCISIONS

[redacted]

Réévaluation de la proportionnalité

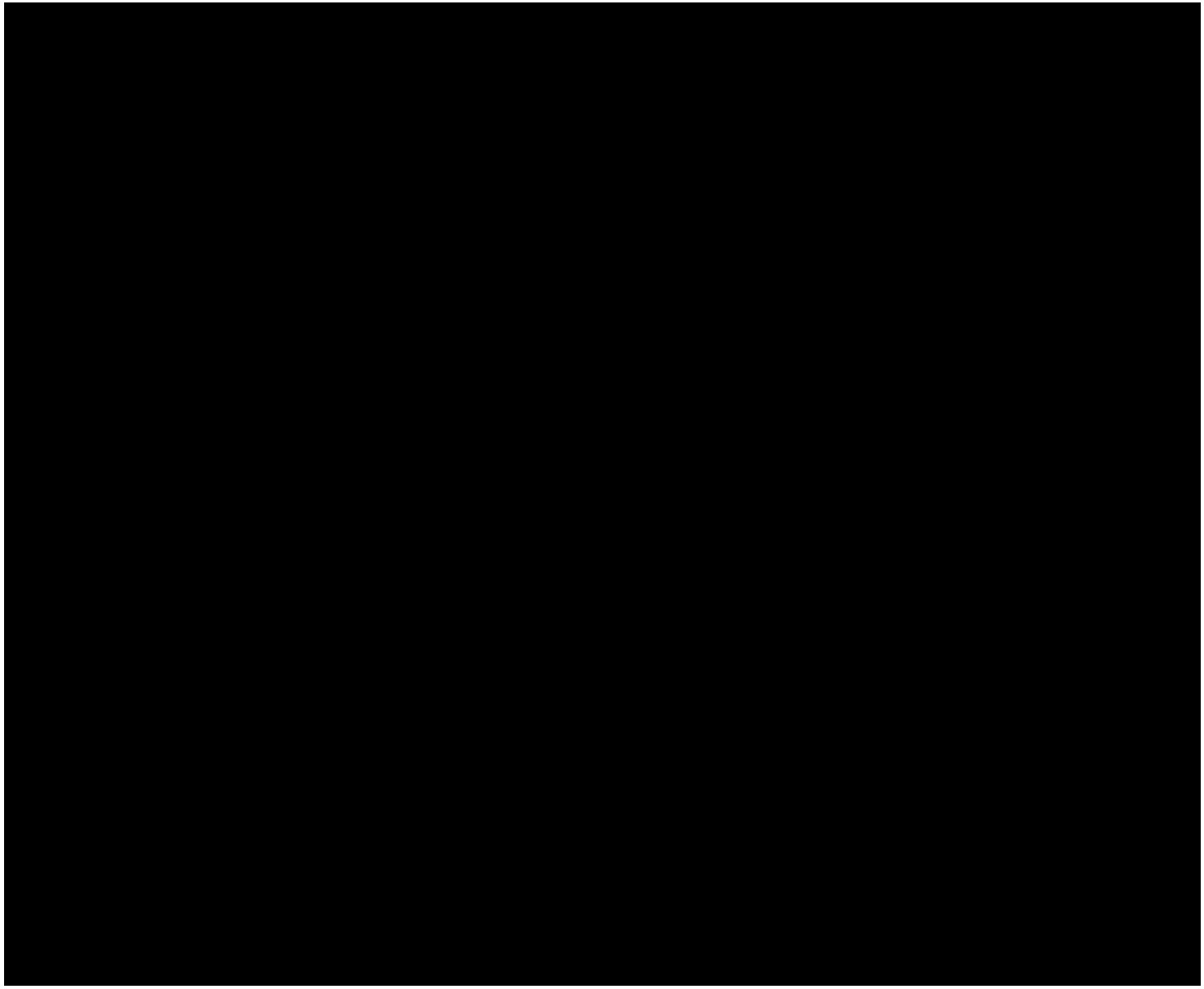
SUITES À DONNER AU PROJET EN FONCTION DE L'ANALYSE

☒ Poursuite sans modification ☐ Poursuite avec modifications ☐ Abandon ou suspension

[redacted]

Il n'y a pas d'impact à la poursuite du projet. Un plan d'action a été identifié afin de mitiger les risques [redacted]

6. PLAN D'ACTION



7. APPROBATION DU RAPPORT ET VERSIONS

Approbation

J’atteste que les informations contenues dans les sections du présent rapport ainsi que les contrôles afférents à ces informations sont fiables et qu’ils correspondent à la situation telle qu’elle se présentait à la date de signature de ce rapport d’évaluation des facteurs relatifs à la vie privée.

[redacted]

Signature de l’autorité responsable

Hippolyte Bafogang Kouongni
Directeur des solutions en ressources financières et matérielles

Date d’approbation : 22 janvier 2025

Date de la prochaine révision prévue : 22 juillet 2025

Ministère
de la Cybersécurité
et du Numérique
Québec

Rapport d'évaluation des facteurs relatifs à la vie privée

Refonte du Système électronique d'appel d'offres (SEAO)

Ministère de la Cybersécurité et du Numérique

Version : octobre 2024

Table des matières

[redacted]

Notes préliminaires

L'EFVP est une démarche préventive et évolutive visant à protéger les RP dans le but de prévenir une atteinte au droit à la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif en matière de respect de la vie privée des clientèles cibles.

Ces facteurs sont, entre autres :

- La conformité du projet à la législation applicable à la protection des RP et le respect des principes qui l'appuient ;
- L'identification des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs impacts ;
- La mise en place de stratégies durant tout le cycle de vie du projet pour éviter la réalisation de ces risques ou réduire l'impact de ceux-ci dans l'éventualité où ils se réalisent.

À noter qu'afin de faciliter la lecture, les acronymes et les définitions ont été regroupés dans des sections qui leur sont dédiées à la fin du présent rapport.

1. Description du projet et de sa portée

Présentation des grandes lignes du projet

Le SEAO est le système électronique d'appel d'offres approuvé par le gouvernement du Québec pour l'application de la LCOP. Il est fourni par un prestataire de services sélectionné par le SCT[1].

Les organismes publics, à titre de donneurs d'ouvrage, assujettis à la LCOP, ainsi que les municipalités et organismes municipaux en vertu de la Loi sur les cités et villes et du Code municipal du Québec, sont tenus d'utiliser le SEAO pour publier leurs avis d'appel d'offres et les renseignements relatifs à leurs contrats, leur permettant de répondre aux exigences de la règlementation en matière de marchés publics.

Les entreprises, à titre de fournisseur, utilisent le SEAO pour consulter les avis publiés, se procurer les documents d'appel d'offres et, s'ils le souhaitent, transmettre leurs soumissions par voie électronique. Le système peut également être utilisé par des organismes privés pour publier des avis d'appel d'offres, principalement lorsque ceux-ci sont subventionnés.

De manière plus générale, le grand public (citoyenne et citoyen) utilise le SEAO à des fins de consultation pour connaitre les besoins des organismes ayant publié des avis d'appel d'offres et pour s'informer, via les informations des contrats, au sujet de l'utilisation des fonds publics.

À la suite d'un appel d'offres public effectué en 2002, le SEAO a été développé par un prestataire de services privé qui depuis en assurait l'hébergement et l'exploitation. Le contrat avec ce prestataire a été renouvelé en décembre 2011 et est arrivé à échéance le 30 novembre 2022. Afin d'assurer la continuité du SEAO à l'échéance de ce contrat, le SCT a fait appel au MCN à titre de gestionnaire de contrat, pour coordonner le projet de refonte du SEAO, ainsi que pour assurer l'hébergement et l'exploitation de la nouvelle solution pour une période de dix (10) ans.

---

[1] Décret numéro 493-2004 (2004, G.O. 2, 2701)

Le projet de refonte du SEAO permet ainsi d'assurer la continuité des services à la fin du contrat avec le prestataire de services privé et marque le détachement avec l'ancien prestataire de service et la prise en charge de l'hébergement et de l'exploitation du SEAO par le gouvernement. De plus, ce projet de refonte a pour objectif le développement d'une solution infonuagique plus évolutive permettant l'ajout de fonctionnalités, l'amélioration des fonctionnalités déjà existantes et l'automatisation de certains processus.

Échéancier du projet

Date de début du projet : 4 juin 2021

Mise en production du SEAO : 6 juin 2024

Mise en production de l'application de veille personnalisée : À déterminer

Énoncé et justification des objectifs motivant le projet

En premier lieu, la refonte du SEAO vise la continuité des services à la fin du contrat avec le prestataire de service privée et est en cohérence avec le plan stratégique 2019-2023 du SCT notamment par rapport à la gestion rigoureuse des ressources de l'État et la performance de l'Administration publique. De plus, en sélectionnant le MCN pour assurer l'hébergement et l'exploitation du SEAO, le SCT réduit la dépendance du gouvernement envers le secteur privé comme recommandé par le Vérificateur général en 2016.

En second lieu, cette refonte vise à créer un environnement infonuagique sécurisé et évolutif en assurant l'application optimale du cadre de gestion des marchés publics pour garantir l'accessibilité aux contrats publics et l'intégrité des processus. Ce nouvel environnement évolutif permet notamment l'ajout de fonctionnalité (ex. : application de veille personnalisée), l'amélioration des fonctionnalités déjà existantes (ex. : développement du site Web considérant l'application du design gouvernemental et du standard d'accessibilité du gouvernement) et la bonification des services offerts par une automatisation accrue de certains processus (ex. : acquisition de biens). Également, la refonte vise l'application des mesures de sécurité robustes en vue d'assurer la confidentialité des données détenues aux fins du SEAO (ex. : cloisonnement des tâches en fonction des rôles établis).

La portée du projet inclut la gestion du changement organisationnelle permettant d'opérer le nouveau système à la suite de sa mise en production. Cette portée a été ajustée en fonction de la consultation du SCT réalisée auprès de certaines parties prenantes au projet tel que les grands donneurs d'ouvrage.

Détermination de la portée de l'évaluation

Cette EFVP[2] porte sur la phase d'exécution du projet de refonte du SEAO et plus spécifiquement sur la circulation des RP nécessaires aux fins de sécurité et de soutien aux opérations ainsi qu'au risque qu'un utilisateur mal informé fournisse des RP qui ne sont pas nécessaires.

[2] Le projet implique la réalisation obligatoire d'une EFVP en vertu de l'article 63.5 de Loi sur l'accès.

2. Rôles et des responsabilités

Intervenants impliqués dans la démarche d'évaluation

Nom, titre	Direction/service	Rôle dans la démarche
Véronique Giroux, Analyste de l'informatique et des procédés administratifs	MCN-SMATNG-DGSCE-DGoSCE	Responsable de la démarche d'EFVP du projet
Mélanie Savard, Conseillère stratégique	MCN-SMATNG-DGSCE-DGoSCE	Soutien-conseil stratégique
David Girouard, Conseiller en architecture fonctionnelle	MCN-SMATNG-DGSCE-DEPSCE-DSISCE	Responsable du développement de la solution
Mélanie Royer, Analyste d'affaires	MCN-SMATNG-DGSCE-DEPSCE	Responsable du développement de la solution
Caroline Bélanger, Responsable produit SEAO	MCN-SMATNG-DGSCE-DEPSCE-DSISCE	Responsable du volet affaires du projet
Nathalie Vidis, Chargée de projet	MCN-SMATNG-DGSCE-DSISCE	Chargée de projet
Wafaa Imlahi Chaer, Conseillère experte en PRP	MCN-SMADPIG-DPAEDNG-DGOPVP	Soutien-conseil en matière de respect de la vie privée et de la PRP
David-Alexandre Girard, Conseiller expert en PRP	MCN-SMADPIG-DPAEDNG-DGOPVP	Soutien-conseil en matière de respect de la vie privée et de la PRP
Diane Laurent, Conseillère experte en PRP	MCN-SMADPIG-DPAEDNG-DGOPVP	Soutien-conseil en matière de respect de la vie privée et de la PRP
Isabelle Lavoie, Conseillère en PRP	MCN-SMADPIG-DPAEDNG-DGOPVP	Soutien-conseil en matière de respect de la vie privée et de la PRP
Denis Nolin, Conseiller en PRP	MCN-SMADPIG-DPAEDNG-DGOPVP	Soutien-conseil en matière de respect de la vie privée et de la PRP
Youri Tacoun, responsable ministériel de la gestion intégrée des risques	MCN-SMCN-DGBSMSG-DSGAAI	Soutien-conseil en matière de gestion de risques
Humberto Diaz, conseiller en architecture de sécurité	MCN-SMASIGC-DGSSI-DArS	Soutien-conseil en SI
Mustapha Ngom, conseiller en architecture de sécurité	MCN-SMASIGC-DGSSI-DArS	Soutien-conseil en SI
Youri Tacoun, responsable ministériel de la gestion intégrée des risques	MCN-SMCN- DGBSMSG-DSGAAI	Soutien-conseil en matière de gestion de risques

3. RP impliqués et ampleur de l'évaluation

Inventaire des RP impliqués

Le projet de refonte du SEAO implique différentes catégories de RP, certains sont des RP confidentiels d'autres sont des RP à caractère public. [redacted]

Catégorisation des RP impliqués dans le projet

Catégories de RP	Personnes visées
RP confidentiel	Grand public
RP à caractère public (non confidentiel)	Membre d'un organisme public ou privé (non authentifié)
RP à caractère public (non confidentiel)	Membre d'un organisme public ou privé (authentifié)

[redacted]

[redacted]

Catégories de RP	Personnes visées	[redacted]

Catégories de personnes qui ont accès aux RP

Rôle	Type d'accès	[redacted]	Explications sur la nécessité pour ces personnes d'avoir accès aux RP
Agent du MESS	Lecture Écriture		Pour le traitement des demandes d'accompagnement
Responsable SI et de la cybersécurité (COCD)	Lecture		Pour la sécurité : prévenir ou détecter des comportements frauduleux et y répondre
Administrateur de l'infrastructure (DGSCE) Exploitant de la solution (CGI)	Lecture		Pour assurer le soutien aux opérations

[redacted]

Québec

[redacted]

[redacted]

4. Moyens mis en place pour répondre à nos obligations et aux principes de PRP

Obligations et principes applicables

Les obligations et les principes de PRP applicables au projet sont notamment prévus dans les divers documents du cadre légal et normatif applicables au projet. L'on y retrouve notamment les documents de gouvernance du MCN concernant la PRP en vigueur ainsi que les différents décrets applicables au projet.

Les principales obligations et principes de PRP[7] qui s'appliquent au projet sont notamment :

- Responsabilité ;
- Détermination des finalités ;
- Limitation de la collecte ;
- Protection dès la conception et par défaut ;
- Consentement ;
- Limitation de l'utilisation, de la communication et de la conservation ;
- Exactitude ;
- Sécurité ;
- Transparence ;
- Droits à l'égard des RP.

Moyens pour répondre à nos obligations et aux principes PRP

Responsabilité

Énoncés	[redacted]
Règles de gouvernance encadrant les RP	
Formation et de sensibilisation en matière de PRP	
Entente et contrat avec les tiers	

[7] Voir notamment les Lignes directrices de l'OCDE régissant la protection de la vie privée.

	[redacted]

Détermination des finalités

Énoncés	
Finalités déterminées avant la collecte et celles-ci sont documentées	[redacted]

Limitation de la collecte

Énoncés	
Légitimité à collecter les RP aux fins déterminées	[redacted]
Limitation de la collecte à ce qui est nécessaire aux fins déterminées	

Protection dès la conception et par défaut

Énoncés	
Protection de la vie privée dès la conception	[redacted]
Protection de la vie privée par défaut	

Consentement

Énoncés	
Type de consentement	[redacted]

Énoncés	[redacted]
Consentement valide	
Exceptions au consentement	
Preuve de consentement	

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

Énoncés	[redacted]
Utilisation et communication aux seules fins déterminées	
Conservation des RP pour la réalisation des fins déterminées	

Exactitude

Énoncé	[redacted]
Mesures raisonnables pour assurer la qualité des RP détenus aux fins du projet	

Sécurité

Énoncés	[redacted]
Mesures de sécurité physiques, techniques et organisationnelles	

Énoncés	[redacted]
Gestion des accès	
Règles de gouvernance concernant l'atteinte à la sécurité, incluant les incidents de confidentialité	

Énoncés	[redacted]

Transparence

Énoncés	[redacted]
Informations fournies aux utilisateurs concernant la PRP	

Droits à l'égard des RP

Énoncés	[redacted]
Demandes d'accès aux RP et de rectification	
Plainte ou commentaire	

5. Identification des risques et des stratégies pour les atténuer

Une analyse a été effectuée pour identifier et évaluer les risques susceptibles de causer une atteinte à la vie privée chez les personnes concernées par le projet de refonte du SEAO. Cette analyse récence également les stratégies et les mesures mises en place pour atténuer ces risques et plus particulièrement ceux dépassant le seuil de tolérance de l'organisation. [redacted]

Une équipe multidisciplinaire a collaboré à la documentation et a participé à l'évaluation des risques [redacted]

Les risques identifiés sont reliés aux étapes du cycle de vie des RP et à la phase de développement et d'exploitation du projet.

- **Collecte** : collecte de RP non nécessaire.
- **Utilisation et communication** : utilisation ou communication des RP à d'autres fins que celles prévues sans consentement ou justification, utilisation ou communication par inadvertance ou à des fins malveillantes.
- **Conservation** : conservation des RP après l'accomplissement des fins pour lesquelles ils ont été recueillis ou utilisés.
- **Destruction** : destruction non sécuritaire ou incomplète (non irréversible).

Analyse des risques d’atteinte à la vie privée

#	Description du risque	[redacted]
1	**Collecte de RP non nécessaire**	

#	Description du risque	[redacted]
2	**Utilisation et communication de RP à d'autres fins que celles prévues sans consentement ou sans justification** **(Volontairement, par inadvertance ou à des fins malveillantes)**	
3	**Conservation des RP après l'accomplissement des fins pour lesquelles ils ont été recueillis ou utilisés**	

[redacted]

#	Description du risque
	(Non-destruction après le délai de conservation)
4	**Destruction non-sécuritaire ou incomplète (non-irréversible)**

Démonstration que le projet est proportionné aux objectifs et aux risques d'atteinte à la vie privée

Au terme de cette analyse, il est possible de conclure que tous les RP impliqués dans le projet sont nécessaires et que les objectifs poursuivis par le projet sont proportionnels aux risques d'atteinte à la vie privée engendrés par celui-ci.

[redacted]

Suites à donner au projet en fonction de l'analyse

☒ Poursuite sans modification ☐ Poursuite avec modifications ☐ Abandon ou suspension

6. Plan d’action

La vérification en vue d’assurer de la mise en œuvre des moyens mis en place pour respecter nos obligations et les principes PRP, d’assurer le suivi de l’analyse de risques en matière de vie privée et des stratégies retenues pour éviter ces risques ou les réduire efficacement sera assurée par l’équipe responsable du projet.

7. Approbation du rapport et versions

Le rapport d'EFVP est un document qui sert à documenter et à consolider les résultats de notre évaluation. Il pourra être mis à jour pour exposer tout changement significatif dans la phase de réalisation du projet ou tout élément s'appliquant à celui-ci et qui ont un impact sur la vie privée des personnes concernées.

Approbation

J'atteste que les informations contenues dans les sections du présent rapport ainsi que les contrôles afférents à ces informations sont fiables et qu'ils correspondent à la situation telle qu'elle se présentait à la date de signature de ce rapport d'évaluation des facteurs relatifs à la vie privée.

Signature de l'autorité responsable

[Nom]

[Titre]

Date d'approbation : *Cliquez ou appuyez ici pour entrer une date.*

Date de la prochaine révision prévue : *Cliquez ou appuyez ici pour entrer une date.*

Journalisation des mises à jour de l'évaluation

Date	Responsable	Modifications
		Création

Cadre légal et normatif

Document	Émetteur ou provenance	Version
Cadre de gouvernance et de gestion de la sécurité de l'information	MCN	2022-03-29
Calendrier de conservation	MCN	S.O.
Décret numéro 493-2004	MCE	2004-05-26
Directive sur la gestion et la classification des actifs informationnels	MCN	2023-02-17
Directive sur la gestion des menaces, des vulnérabilités, des incidents de sécurité de l'information et des incidents impliquant des renseignements personnels	MCN	2023-02-17
Directive sur la gestion des accès physique	MCN	2023-02-17
Directive sur la gestion des identités et des droits d'accès aux actifs informationnels du ministère de la cybersécurité et du numérique	MCN	2022-09-26
Directive sur la conformité des services en matière de sécurité de l'information	MCN	2023-02-17
Directive sur la sécurité applicative	MCN	2023-10-31
Directive sur la sécurité des réseaux et des télécommunications	MCN	2023-10-31
Directive sur la sécurité de l'information des ressources humaines	MCN	2023-10-31
Directive sur les obligations relatives à la confidentialité et à la déclaration de conflit d'intérêts	MCN	2023-06-28
Directive sur l'encadrement des exigences de sécurité vis-à-vis des tiers	MCN	2023-02-17
Mesures minimales de sécurité au regard des données lors de l'utilisation de solutions technologiques	MCN	2023-02-01
L'éthique dans la fonction publique québécoise (ISBN 2-550-40764-4)	MCE	2003
Loi concernant la cadre juridique des technologies de l'information (RLRQ, c. C-1.1)	MCE	Mise à jour en continu — Publications du Québec
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03)	MCE	Mise à jour en continu — Publications du Québec
Loi sur les archives (RLRQ, c. A-21.1)	MCE	Mise à jour en continu — Publications du Québec

Document	Émetteur ou provenance	Version
Loi sur les contrats des organismes publics (RLQQ, c. C-65.1)	MCE	2022
Politique-cadre en matière de télétravail pour les employés de la fonction publique	SCT	2022-04-04
Politique de sécurité de l'information	MCN	2023-06-01
Politique sur les conflits d'intérêts	MCN	2023-06-28
Procédure de gestion des incidents de confidentialité	SRIDAI du MCE	S.O.
Processus de gestion de l'identité et des droits d'accès	MCN	2023-11
Règles de sécurité de l'information destinées au personnel du ministère de la Cybersécurité et du Numérique	MCN	S.O.
Processus de gestion des plaintes et commentaires – Système électronique d'appel d'offres	MCN	2024-08
Règles de sécurité destinées aux ressources externes	MCN	S.O.
Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, c. A-2.1, r. 2)	MCE	Mise à jour en continu — Publications du Québec
Règles relatives à la gestion des projets en ressources informationnelles	MCE	2022-06-22

Acronymes

CGCD	Centre gouvernemental de cyberdéfense
CSIPRPC	Comité sur la SI, la PRP et la continuité
DArS	Direction de l'architecture de sécurité
DEPSCE	Direction de l'évolution des produits des solutions citoyennes et entreprises
DGOPVP	Direction du gouvernement ouvert et de la protection de la vie privée
DGoSCE	Direction de la gouvernance des solutions citoyennes et entreprises
DGSCE	Direction générale des solutions citoyennes et entreprises
DGSSI	Direction générale de la sécurité des services et de l'information
DPAEDNG	Direction principale de l'architecture d'entreprise et des données numériques gouvernementales
DSISCE	Direction des systèmes d'information des solutions citoyennes et entreprises
EFVP	Évaluation des facteurs relatifs à la vie privée
LCOP	Loi sur les contrats des organismes publics
MCE	Ministère du Conseil exécutif
MCN	Ministère de la Cybersécurité et du Numérique
PRP	Protection des renseignements personnels
RP	Renseignement(s) personnel(s)
RPRP	Responsable de la protection des renseignements personnels
SAG	Service d'authentification gouvernementale
SCT	Secrétariat du Conseil du trésor
SI	Sécurité de l'information
SEAO	Système électronique d'appel d'offres
SMATNG	Sous-ministériat adjoint à la transformation numérique gouvernementale
SMADPIG	Sous-ministériat adjoint au dirigeant principal de l'information et à la gouvernance du numérique
SMASIGC	Sous-ministériat adjoint à la sécurité de l'information gouvernemental et à la cybersécurité

Définitions

Sujet	Définition
Consentement	Action de donner son accord, son acceptation, son autorisation à une action, à un projet.
Authentification	L'authentification est un processus de validation permettant d'assurer que la personne qui entend utiliser ou autrement bénéficier d'un service est bien celle qu'elle prétend être. Elle vise à donner l'assurance qu'une telle personne conserve le contrôle des justificatifs lui permettant l'accès au service concerné et que ceux-ci n'ont pas été compromis.
RP	Toute information qui concerne une personne physique et qui permet de l'identifier directement ou indirectement.
Utilisateur	Une personne (ou son représentant) qui utilise les services créés et déployés dans le cadre du projet.