

FORMULAIRE DU GUIDE DES BONNES PRATIQUES EN IA

DISPOSITIONS DE LA LOI 25 ET
BONNES PRATIQUES



CENTRE
DE RECHERCHE
EN DROIT
PUBLIC



OBSERVATOIRE INTERNATIONAL
SUR LES IMPACTS SOCIÉTAUX
DE L'IA ET DU NUMÉRIQUE

Produit avec le soutien financier des Fonds de recherche du Québec



Fonds de recherche – Nature et technologies
Fonds de recherche – Santé
Fonds de recherche – Société et culture

ISBN : 978-2-925138-36-5
DOI: 10.61737/PUPD4808

INTRODUCTION

Ce document, qui se présente sous la forme d'un formulaire, propose une liste de questions relatives à certaines obligations légales découlant de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels¹ (« Loi 25 ») ainsi qu'aux bonnes pratiques pour les entreprises et les organismes publics qui utilisent l'IA. Tant les obligations explicitement identifiées dans la Loi 25 que celles que nous avons mis de l'avant dans le présent *Guide* sont mises en perspective dans ce formulaire.

Le formulaire est divisé en sept sections reprenant les sept principes relatifs à l'utilisation des données et à la protection des renseignements personnels dans un contexte d'IA formulés dans le présent *Guide*. Il permet au répondant d'évaluer sa conformité aux principales obligations visant à assurer une circulation responsable des données.

Le formulaire a été construit selon un effet miroir dans lequel certaines des obligations légales de la Loi 25 se reflètent sur les bonnes pratiques en matière d'IA.

L'utilisation du *Guide des bonnes pratiques en intelligence artificielle* est essentielle pour répondre au présent formulaire puisqu'il fournit un appui pour comprendre et mettre en œuvre les bonnes pratiques.

¹ Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25

1. Responsabilité

1.1 Personne responsable

Obligations légales			Bonnes pratiques		
			Un ou une responsable en IA a-t-il/elle été nommé(e) ?	Oui	Non
Nom du ou de la personne exerçant la fonction de responsable de la protection des renseignements personnels (art. 8 LAI / art. 3.1 LSP)	(Inscrire)		Nom du ou de la personne ayant la plus haute autorité dans l'organisation (Si oui à la réponse précédente)	(Inscrire)	
Le titre et les coordonnées du ou de la responsable des renseignements personnels ont-ils été publiés sur le site internet de l'organisation ou par tout autre moyen approprié ? (art. 17 LAI / art. 3.1 LSP)	Oui	Non	Le titre et les coordonnées du ou de la responsable en IA ont-ils été publiés sur le site internet de l'organisation ou par tout autre moyen approprié ?	Oui	Non
Précisions / observations :					

1.2 Gouvernance, expertise et documentation

Obligations légales			Bonnes pratiques		
Des règles, politiques et pratiques encadrant la gouvernance et la protection des renseignements personnels ont-elles été établies et publiées (ou rendues accessibles par tout autre moyen) ? (art. 63.3 LAI / art. 3.2 LSP)	Oui	Non	Les politiques, pratiques et mesures entourant la protection des renseignements personnels sont-elles alignées à une stratégie de gouvernance et de gestion de risque d'IA ?	Oui	Non
Un comité sur l'accès à l'information et la protection des renseignements personnels a-t-il été constitué ? (Obligatoire s'il s'agit d'un organisme public) (art. 8.1 LAI)	Oui	Non	Des équipes avec des expertises variées pour les projets nécessitant l'utilisation d'IA ont-elles été mises en place ?	Oui	Non

Votre organisme public remplit-il ses obligations de documentation (inscription des communications et entente de collectes de renseignements personnels et mise à jour d'un inventaire)? (art. 67.3, 76 LAI)	Oui	Non	Des registres détaillés de chaque projet en IA sont-ils tenus ?	Oui	Non
	N/A				
			Des formations concernant la conception, le fonctionnement et le déploiement d'un SIA sont-elles prévues ?	Oui	Non
			Des experts ont-ils été consultés afin d'obtenir une évaluation du SIA ?	Oui	Non
Précisions / observations :					

1.3 Évaluation des facteurs relatifs à la circulation des données

Obligations légales			Bonnes pratiques		
Une évaluation des facteurs relatifs à la vie privée (ÉFVP) a-t-elle été effectuée ? (art. 63.5, 64, 67.2.1, 68 et 70.1 LAI / art. 3.3, 17 et 21 LSP)	Oui	Non	Une évaluation des facteurs relatifs à la circulation des données pour l'IA a-t-elle été effectuée ?	Oui	Non
La réalisation de l'ÉFVP s'avère-t-elle proportionnée à la sensibilité des renseignements personnels, à la finalité de leur utilisation, ainsi qu'à leur quantité, répartition et support ? (Si oui à la question précédente)(art. 63.5 LAI / art. 3.3 LSP)	Oui	Non	L'évaluation a-t-elle permis d'identifier des risques au droit à la vie privée et des manières d'atténuer ces derniers ?	Oui	Non
			Des consultations ont-elles été effectuées dès le début de la conception du SIA (responsable en IA, fournisseurs de modèles, individus concernés, parties prenantes, etc.) ?	Oui	Non

	Souhaitez-vous mettre en place des évaluations régulières et une surveillance des données dès le départ et tout au long du cycle de vie du SIA ?	Oui	Non
Précisions / observations :			

2. Justification sociale

2.1 Objectif suffisamment important

Obligations légales			Bonnes pratiques		
Le recueil des renseignements personnels est-il nécessaire aux fins déterminées avant la collecte ou à l'exercice des attributions d'un organisme ou à la mise en œuvre d'un programme dont il a la gestion ? (art. 64 LAI / art. 5 LSP)	Oui	Non	Les avantages rendus possibles par le SIA seront-ils suffisamment importants pour justifier l'utilisation des données ?	Oui	Non
L'intérêt et les fins relatifs au recueil des renseignements personnels ont-ils été choisis avant la collecte ? (art. 64 LAI / art. 4 LSP)	Oui	Non	Avez-vous déterminé un intérêt et des justifications spécifiques à chaque phase du cycle de vie d'un SIA ?	Oui	Non
	Oui	Non	Avez-vous documenté et publié l'intérêt et les fins déterminées de votre projet ?	Oui	Non
Précisions / observations :					

2.2 Proportionnalité

Obligations légales			Bonnes pratiques		
L'ÉFVP est-elle obligatoire dans votre projet afin de vous assurer de la proportionnalité de la collecte de renseignement personnel ? (art. 63.5, 64, 67.2.1, 68 et 70.1 LAI / art. 3.3, 17 et 21 LSP)	Oui	Non	Avez-vous effectué une évaluation de facteurs relatifs à la circulation des données afin de déterminer la proportionnalité des risques et des bénéfices de l'utilisation d'un SIA ?	Oui	Non
			Avez-vous identifié la quantité minimale de renseignements personnels nécessaires aux fins déterminées pour le fonctionnement du SIA ?	Oui	Non
Précisions / observations :					

2.3 Utilisation et conservation

Obligations légales			Bonnes pratiques		
Les renseignements personnels de votre projet sont-ils utilisés à d'autres fins que celles pour lesquelles ils ont été recueillis ? (art. 65.1 LAI / art. 12 LSP)	Oui	Non	Vous êtes-vous assuré que le SIA performe de la manière attendue et soit suffisamment précis ? (Ceci vise à vous assurer qu'un renseignement personnel est utilisé conformément aux fins prévues)	Oui	Non
Les nouvelles finalités respectent-elles les obligations légales (consentement de la personne concernée ou fin compatible avec la finalité initiale, etc.) ? (Si oui à la question précédente) (art. 65.1 LAI / art. 12 LSP)	Oui	Non			
			Avez-vous procédé à l'étiquetage des données ?	Oui	Non

S'il s'agit d'une fin compatible avec la finalité initiale, celle-ci a-t-elle un lien pertinent et direct avec les fins pour lesquelles les renseignements ont été recueillis ? (Si oui à la question précédente)(art. 65.1 LAI / art. 12 LSP)	Oui	Non	Les données d'entraînement ont-elles une fin compatible avec celles pour lesquelles elles ont été initialement recueillies ?	Oui	Non
Un délai de conservation est-il prévu par la loi ?	Oui	Non			
Lorsque les fins pour lesquelles les renseignements personnels ont été recueillis ou utilisés sont accomplies, ceux-ci seront (art. 73 LAI / art. 23 LSP):	Détruit Anonymisé		Avez-vous procédé à un test d'intrusion afin d'évaluer le risque de réidentification ? (Ne répondre que si une anonymisation est prévue)	Oui	Non
Précisions / observations :					

3. Transparence

3.1 Information générale

Obligations légales			Bonnes pratiques		
Les renseignements personnels sont-ils recueillis par un moyen technologique ? (art. 63.4 LAI / art. 8.2 LSP)	Oui	Non			
Une politique de confidentialité a-t-elle été publiée ? (art. 63.4 LAI / art. 8.2 LSP)	Oui	Non	Prévoyez-vous de faire des publications contenant de l'information générale sur le SIA ?	Oui	Non
La politique de confidentialité est-elle rédigée en des termes simples et clairs ? (art. 63.4 LAI / art. 8.2 LSP)	Oui	Non	L'explication relative au traitement des renseignements personnels par un SIA est-elle compréhensible ?	Oui	Non

	Des recours sont-ils prévus en cas de manque de transparence de votre organisation quant à l'utilisation du SIA ?	Oui	Non
Précisions / observations :			

3.2 Accès aux renseignements

Obligations légales			Bonnes pratiques		
Avez-vous informé la personne concernée de son droit d'accès et de rectification prévus par la loi ? (art. 65 LAI / art. 8 LSP)	Oui	Non	Avez-vous prévu de faire un portail permettant aux personnes concernées d'avoir accès à leur profil et aux informations les concernant ?	Oui	Non
Êtes-vous en mesure d'informer la personne concernée de l'existence d'un renseignement personnel la concernant et de lui permettre d'en recevoir communication ? (art. 83 LAI / art. 27 LSP)	Oui	Non			
Dans le cas où les renseignements personnels sont informatisés, peuvent-ils être communiqués sous la forme d'une transcription écrite et intelligible ? (art. 84 LAI / art. 27 LSP)	Oui	Non			
Dans le cas où les renseignements personnels sont informatisés, peuvent-ils être communiqués dans un format technologique structuré et couramment utilisé ? (art. 84 LAI / art. 27 LSP)	Oui	Non			
Précisions / observations :					

3.3 Usage de certaines technologies

Obligations légales			Bonnes pratiques		
Lors du recueil de leurs renseignements personnels, les personnes concernées seront-elles informées du recours à une technologie comprenant des fonctions permettant de les identifier, localiser ou d'effectuer un profilage de celles-ci? (art. 65.0.1 LAI / art. 8.1 LSP)	Oui	Non			
La personne concernée sera-t-elle informée avant ou au moment où une décision fondée exclusivement sur un traitement automatisé est prise? (art. 65.2 LAI / art. 12.1 LSP)	Oui	Non			
Précisions / observations :					

4. Sécurité

4.1 Mesures de sécurité adaptées

Obligations légales			Bonnes pratiques		
Des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits ont-elles prises? (art. 63.1 LAI / art. 10 LSP)	Oui	Non	Des mesures de sécurité techniques informatiques relatives à la sécurité et à l'exactitude des renseignements personnels traités par un SIA sont-elles prévues?	Oui	Non
Ces mesures de sécurité sont-elles raisonnables compte-tenu, notamment, de la sensibilité des renseignements personnels, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support? (art. 63.1 LAI / art. 10 LSP)	Oui	Non			

Les règles encadrant la manière d'assurer la protection des renseignements personnels sont-elles publiées et accessibles à tous ? (art. 63.3 LAI / art. 3.2 LSP)	Oui	Non	Avez-vous documenté vos mesures de sécurité organisationnelles relatives au SIA ?	Oui	Non
Des mesures raisonnables sont-elles prévues pour diminuer les risques et éviter un (nouvel) incident de confidentialité ? (art. 3.5 à 3.7 LAI / art. 63.8 à 63.10 LSP)	Oui	Non	Une réévaluation régulière des facteurs de risques relatifs aux renseignements personnels (comme les cyberattaques) est-elle prévue ?	Oui	Non
Des mesures permettant d'aviser les personnes concernées par un incident de confidentialité sont-elles prévues ? (art. 3.5 LAI / art. 63.8 LSP)	Oui	Non			
L'organisation a-t-elle prévu un registre des incidents de confidentialité ? (art. 3.8 LAI / art. 63.11 LSP)	Oui	Non			
			Avez-vous procédé à une évaluation de facteurs relatifs à la circulation des données afin d'établir le niveau de mesures de sécurité nécessaires pour l'utilisation du SIA ?	Oui	Non
			Avez-vous identifié les préjudices potentiels causés par un défaut ou une attaque à un modèle d'IA ?	Oui	Non
			Avez-vous identifié les types de vulnérabilités auxquelles un SIA est exposé (pollution de données, infrastructure physique du système, cyberattaques, etc.) ?	Oui	Non
			Avez-vous déterminé une manière de valider la performance du modèle de SIA lorsque de nouvelles données sont ajoutées ?	Oui	Non
			Avez-vous établi des méthodes d'évaluation pour vérifier si le modèle est fiable et reproductible ?	Oui	Non

	Avez-vous prévu une politique d'approvisionnement d'IA avec un niveau suffisant en termes de partage d'information ?	Oui	Non
	Avez-vous déterminé la durée entre les mises à jour des paramètres de sécurité selon les limites et besoins du SIA ?	Oui	Non
	Vos mesures de sécurité organisationnelles incluent-elles des formations sur les risques d'incidents de sécurité relatifs aux renseignements personnels traités par un SIA ?	Oui	Non
Précisions / observations :			

4.2 Données d'entraînement et cyberattaques

Obligations légales	Bonnes pratiques		
	Tenez-vous un registre documentant les mouvements et le stockage des données ?	Oui	Non
	Appliquez-vous des techniques de dépersonnalisation aux données d'entraînement avant qu'elles ne soient partagées ?	Oui	Non
	Les logiciels et le matériel informatique sont-ils adaptés face aux risques d'utilisation de codes standards d'apprentissage automatiques en open source ? (Répondre si vous utilisez de tels codes)	Oui	Non
	Prévoyez-vous une ligne de conduite sécuritaire dès la conception du SIA qui sépare l'environnement du développement du modèle d'IA du reste de l'infrastructure informatique ?	Oui	Non
	Prévoyez-vous de convertir le langage de programmation du développement dans un format plus sécuritaire lors de la phase de déploiement ?	Oui	Non

	Avez-vous identifié les types de cyberattaques possibles et celles auxquelles le SIA est le plus vulnérable ?	Oui	Non
	Avez-vous prévu des procédures de gouvernance en cas d'urgence ou d'échec du système ou de cyberattaque ?	Oui	Non
Précisions / observations :			

5. Explicabilité

5.1 Proportionnalité

Obligations légales			Bonnes pratiques		
La personne concernée sera-t-elle informée des fins auxquelles ces renseignements sont recueillis, des moyens par lesquels les renseignements sont recueillis, de ses droits d'accès et de rectification ainsi que de son droit de retirer son consentement à la communication ou l'utilisation des renseignements recueillis ? (art. 65 LAI / art. 8 LSP)	Oui	Non	Vos raisons, paramètres et facteurs communiqués à la personne concernée incluent-ils suffisamment d'informations permettant de comprendre la logique sous-jacente de la décision d'un SIA ?	Oui	Non
Le consentement demandé à la personne concernée a-t-il été manifeste, libre, éclairé et donné à des fins spécifiques ? (art. 53.1 LAI / art. 14 LSP)	Oui	Non			
Avez-vous prévu d'effectuer toutes vos communications en des termes simples et clairs ?	Oui	Non	La communication des paramètres et des facteurs sera-t-elle faite en des termes simples et clairs ?	Oui	Non
			Prévoyez-vous d'expliquer à la personne concernée la conception des fonctionnalités, des attributs et des modèles du SIA ainsi que l'utilisation des renseignements personnels ?	Oui	Non

	Avez-vous développé une politique interne sur l'explicabilité ?	Oui	Non
	Avez-vous inclus le principe d'explicabilité dans la conception, dès le début du projet et à chacune des phases de développement du SIA ?	Oui	Non
	Avez-vous évalué quelle est la compréhension du SIA par les personnes concernées ?	Oui	Non
	Prévoyez-vous de publier et de partager le code source ou le modèle du SIA ?	Oui	Non
	Prévoyez-vous d'offrir une licence sur les données du SIA ? (Si non à la question précédente)	Oui	Non
	Prévoyez-vous de publier les métadonnées du modèle du SIA ? (Si non aux questions précédentes)	Oui	Non
Précisions / observations :			

6. Exactitude, droit de rectification et droit de révision

6.1 Exactitude

Obligations légales			Bonnes pratiques		
Les renseignements personnels détenus sont-ils exacts, complets et à jour pour l'utilisation aux fins déterminées ? (art. 72 LAI / art. 11 et 71 LSP)	Oui	Non	Les renseignements personnels utilisés pour produire des inférences, prédictions et évaluations sont-ils exacts, mis à jour, complets et non équivoques ?	Oui	Non
			Avez-vous documenté et enregistré ces mesures ?	Oui	Non
			Avez-vous établi des mesures de traçabilité des données pour identifier le renseignement personnel qui a été utilisé afin de rendre une décision ?	Oui	Non

	Avez-vous mis en place des outils de gestion de préférences en matière de vie privée à la disposition des personnes concernées ?	Oui	Non
	Prévoyez-vous la mise à jour et la révision régulière des données ?	Oui	Non
	Envisagez-vous de vous attarder sur la compréhension des facteurs pouvant nuire à la qualité et à l'exactitude des données ?	Oui	Non
	Prévoyez-vous de tenir un registre des décisions erronées à cause de renseignements personnels inexacts, incomplets ou équivoques ?	Oui	Non
Précisions / observations :			

6.2 Droit de rectification

Obligations légales			Bonnes pratiques		
Avez-vous envisagé les meilleures façons de procéder à la rectification d'un renseignement personnel lorsqu'une personne concernée le demande conformément à la loi ? (art. 65.2, 89 à 93, 94 et 98 LAI / art. 8, 12.1, 16, 19, 28, 28.1, 29, 30, 32 à 36, 78, 79 LSP)	Oui	Non	Avez-vous incorporé des fonctions permettant un retrait ou une rectification des renseignements personnels sans altérer de façon majeure le modèle ?	Oui	Non
			Avez-vous mis en place des canaux de communication permettant aux personnes concernées de donner des commentaires ou de poser des questions en lien avec leurs renseignements personnels ?	Oui	Non
Précisions / observations :					

6.3 Révision de décision exclusivement automatisée et sans intervention humaine

Obligations légales			Bonnes pratiques		
La personne concernée sera-t-elle informée de l'utilisation de ses renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci ? (art. 12.1 LAI / art. 65.2 LSP)	Oui	Non	Les renseignements personnels utilisés par le SIA afin de produire une décision automatisée, les observations additionnelles de la personne concernée ainsi que les facteurs externes additionnels ont-ils été analysés ?	Oui	Non
La personne concernée pourra-t-elle être informée, sur demande, des renseignements personnels utilisés, de son droit de les faire rectifier ainsi que des raisons et des principaux facteurs paramètres ayant mené à la décision ? (art. 12.1 LAI / art. 65.2 LSP)	Oui	Non	Les décisions fondées exclusivement sur un traitement automatisé et les révisions de ces décisions sont-elles équitables, justes et non-discriminatoires ?	Oui	Non
La personne concernée aura-t-elle l'occasion de présenter ses observations à un membre du personnel en mesure de réviser la décision ? (art. 12.1 LAI / art. 65.2 LSP)	Oui	Non	Avez-vous facilité le processus de révision de décision en offrant une manière simple de contester la décision et de présenter ses observations ?	Oui	Non
			Les données recueillies sur les révisions effectuées seront-elles régulièrement surveillées et analysées ?	Oui	Non
			Prévoyez-vous la tenue d'un registre des demandes de révision de décisions fondées exclusivement sur un traitement automatisé ?	Oui	Non
Précisions / observations :					

6.4 Membres du personnel chargés des révisions

Obligations légales	Bonnes pratiques		
	Les membres du personnel pourront-ils faire des révisions significatives et renverser des décisions automatisées ?	Oui	Non
	Les membres de votre personnel recevront-ils une orientation, une formation et un support adéquat relativement aux résultats du SIA ?	Oui	Non
	Des mécanismes relatifs au biais d'automatisation des membres du personnels seront-ils prévus à chaque phase du cycle de vie du SIA ?	Oui	Non
	Un comité d'évaluation indépendant sera-t-il mis sur pied ?	Oui	Non
Précisions / observations :			

7. Non-discrimination

Obligations légales			Bonnes pratiques		
La Charte québécoise, en matière de non-discrimination, est-elle respectée ? (art. 10 Charte)	Oui	Non	Le terme de discrimination dans le contexte spécifique du SIA est-il clairement défini ?	Oui	Non
			Les résultats du SIA sont-ils justes et équitables ?	Oui	Non
			Le responsable en IA a-t-il mis en place des mesures et politiques conformes à l'état de l'art ?	Oui	Non
			Des formations éducatives sur les risques de discrimination d'un SIA ont-elles été offertes à vos membres du personnel responsables de la création et du bon fonctionnement du SIA ?	Oui	Non

	Est-il prévu de surveiller et d'évaluer régulièrement le SIA tout au long de son cycle de vie afin de prévenir des résultats discriminatoires ?	Oui	Non
	Avez-vous pris en compte le potentiel de discrimination dès le début de la conception du SIA ?	Oui	Non
	Si oui à la question précédente, des mesures efficaces ont-elles été prises ?	Oui	Non
	Avez-vous mis en place un système de signalement de problèmes liés à la discrimination ou à la mauvaise performance du SIA ?	Oui	Non
Précisions / observations :			



CENTRE
DE RECHERCHE
EN DROIT
PUBLIC



OBSERVATOIRE INTERNATIONAL
SUR LES IMPACTS SOCIÉTAUX
DE L'IA ET DU NUMÉRIQUE