Politique de gouvernance des renseignements personnels

Forge Tech inc. — politique et pratiques encadrant la protection des renseignements personnels

Obligation en vigueur depuis septembre 2023 · Version 1.0 · Août 2026

1. OBJET ET PORTÉE

La présente politique établit le cadre de gouvernance des renseignements personnels de Forge Tech inc. Elle s'applique :

- à toute personne agissant pour Forge Tech — dirigeant, employé, pigiste, sous-traitant, stagiaire ;
- à tous les renseignements personnels détenus par l'entreprise, quel qu'en soit le support ;
- à l'ensemble du cycle de vie de ces renseignements : collecte, utilisation, communication, conservation et destruction.

2. RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Titulaire	**Guillaume Régimbald**, fondateur et dirigeant
Coordonnées publiées	info@forge-tech.ca · **1 418 935-1300**
Autorité	Il exerce la plus haute autorité de l'entreprise en matière de protection des renseignements personnels et rend compte directement au conseil d'administration

Ses fonctions : approuver la présente politique et ses mises à jour ; approuver les évaluations des facteurs relatifs à la vie privée ; agir comme commandant en cas d'incident ; tenir les registres exigés ; traiter les demandes des personnes concernées et les plaintes ; assurer la formation du personnel ; réviser annuellement le cadre de gouvernance.

> La désignation formelle du responsable, ainsi que la délégation en cas d'absence, font l'objet d'un document distinct conservé au registre corporatif.

3. PRINCIPES DIRECTEURS

1. **Nécessité** — nous ne recueillons que les renseignements nécessaires à des fins déterminées, avant la collecte.
2. **Transparence** — nous informons les personnes de l'usage prévu, en termes simples, au moment de la collecte.
3. **Consentement** — libre, éclairé, donné à des fins spécifiques, et exprès lorsque les renseignements sont sensibles.
4. **Minimisation** — nous limitons les accès internes au strict nécessaire selon les fonctions de chacun.
5. **Exactitude** — nous corrigeons sans délai tout renseignement inexact porté à notre attention.
6. **Sécurité par défaut** — les paramètres les plus protecteurs s'appliquent par défaut dans nos produits.
7. **Durée limitée** — nous détruisons ou anonymisons les renseignements dont la finalité est accomplie.
8. **Responsabilité démontrable** — nous documentons nos décisions afin de pouvoir en rendre compte.

4. RÔLES INTERNES ET GESTION DES ACCÈS

Fonction	Accès aux renseignements personnels	Encadrement
Dirigeant et responsable	Accès complet, requis pour l'exploitation et le soutien	Journalisation de tous les accès aux données clients
Personnel de soutien à la clientèle	Accès limité au dossier du client qui demande de l'aide, pour la durée de la demande	Entente de confidentialité signée ; formation obligatoire ; accès révoqué au départ
Pigiste ou sous-traitant technique	Aucun accès aux données réelles ; travaux effectués sur données fictives	Entente de confidentialité et cession de propriété intellectuelle signées avant le premier accès
Comptable et avocat externes	Accès limité aux pièces nécessaires à leur mandat	Secret professionnel

Règles constantes : comptes nominatifs — aucun compte partagé ; authentification à deux facteurs pour tout accès administratif ; révocation des accès **le jour même** de la fin d'un lien d'emploi ou de mandat ; revue des accès au moins une fois par année.

5. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Une évaluation est obligatoire **avant** :

1. tout projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels ;

2. toute communication de renseignements personnels **hors du Québec** ;
3. toute communication de renseignements personnels à un tiers sans consentement, dans les cas permis par la loi.

L'évaluation est proportionnée à la sensibilité des renseignements, à leur finalité et à leur quantité. Elle est consignée et approuvée par le responsable avant la mise en œuvre du projet. Le modèle et le registre figurent dans un document distinct.

6. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Tout incident, réel ou soupçonné, est signalé **immédiatement** au responsable. La marche à suivre — confinement, évaluation du risque de préjudice sérieux, avis à la Commission d'accès à l'information et aux personnes concernées, avis aux clients dans les 24 heures, inscription au registre conservé 5 ans — est décrite dans la *Procédure de réponse aux incidents de confidentialité*.

7. TRAITEMENT DES DEMANDES ET DES PLAINTES

Type de demande	Délai de réponse	Frais
Accès aux renseignements	30 jours	Aucun (frais raisonnables de transcription possibles, avisés d'avance)
Rectification	30 jours	Aucun
Retrait du consentement	Sans délai	Aucun
Portabilité (renseignements informatisés)	30 jours	Aucun
Plainte	Accusé de réception sous 5 jours ouvrables, réponse motivée sous 30 jours	Aucun

Un refus est toujours motivé par écrit, avec mention de la disposition légale invoquée et du droit de porter plainte à la **Commission d'accès à l'information du Québec**.

8. CONSERVATION ET DESTRUCTION

Les durées de conservation et les méthodes de destruction sécuritaire sont établies dans la *Politique de conservation et de destruction des documents*. Aucun renseignement personnel n'est conservé « au cas où ».

9. RECOURS À DES PRESTATAIRES DE SERVICES

Avant de confier des renseignements personnels à un fournisseur, Forge Tech :

1. vérifie que le fournisseur offre des garanties de protection adéquates ;
2. conclut une **entente écrite** précisant les mesures de protection, la localisation des renseignements, l'interdiction d'usage à d'autres fins et les obligations en cas d'incident ;
3. réalise une évaluation des facteurs relatifs à la vie privée si le traitement se fait hors du Québec ;
4. inscrit la communication au registre approprié.

10. RENSEIGNEMENTS CONFIÉS PAR LES CLIENTS

Pour les renseignements hébergés dans la plateforme par ses clients, Forge Tech agit comme **prestataire de services** et non comme responsable. Ses engagements sont formalisés dans l'*Entente de traitement des renseignements personnels* signée avec chaque client, qui prévoit notamment l'hébergement au Québec, l'interdiction de tout usage autre que la prestation du service, l'interdiction d'entraîner des modèles d'intelligence artificielle avec ces données, et le respect du secret professionnel des clients qui y sont assujettis.

11. FORMATION ET SENSIBILISATION

Toute personne qui accède à des renseignements personnels reçoit une formation **avant son premier accès**, portant sur la présente politique, la procédure d'incident et les règles d'accès. Un rappel annuel est effectué. La tenue de ces formations est consignée.

12. GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE

1. **L'humain décide** — aucune décision produisant un effet pour une personne n'est prise sans validation humaine.
2. **Aucun entraînement** sur les données des clients.
3. **Traitement local par défaut** pour les renseignements sensibles.
4. **Consentement explicite** avant l'activation d'une fonction envoyant du contenu à un fournisseur externe.
5. **Réversibilité** — capacité maintenue de basculer vers un traitement local.

13. RÉVISION

La présente politique est révisée **au moins une fois par année**, ainsi qu'à l'occasion de tout changement législatif, de tout incident significatif ou de tout nouveau projet d'envergure. La date de la dernière révision est indiquée ci-dessous.

14. MANQUEMENTS

Un manquement à la présente politique peut entraîner des mesures disciplinaires pouvant aller jusqu'à la fin du lien d'emploi ou la résiliation du contrat, en plus des recours civils et pénaux prévus par la loi.

Adoptée le	**8 août 2026**
Approuvée par	Guillaume Régimbald, responsable de la protection des renseignements personnels
Version	1.0
Dernière révision	Août 2026
Prochaine révision	Août 2027
Diffusion	Publiée sur forge-tech.ca et remise à toute personne agissant pour l'entreprise

Document généré par Forge Tech · projet à valider par un avocat.