LIVRAISON RIKI

Évaluation des Facteurs relatifs à la Vie Privée

Projet LIVRAISON RIKI — Plateforme de livraison locale

Document : **ÉFVP · Loi 25 du Québec, article 3.3**
Version 1.0 · Rédigé le 06 octobre 2026
Responsable Loi 25 : **Yasser MAKHLOUF**

LIVRAISON RIKI (entreprise en constitution)
131 rue des Flandres, Rimouski (Québec) G5M 0L3, Canada
Tél. : 1-418-509-2069
confidentialite@livraisonriki.com
livraisonriki.com

1. Préambule et contexte juridique

La présente Évaluation des Facteurs relatifs à la Vie Privée (ÉFVP) est réalisée en conformité avec l'**article 3.3 de la Loi sur la protection des renseignements personnels dans le secteur privé** (RLRQ, c. P-39.1), telle que modifiée par la **Loi modernisant des dispositions législatives en matière de protection des renseignements personnels** (ci-après « Loi 25 »). Elle vise à identifier, évaluer et atténuer les risques pour la vie privée des personnes concernées dans le cadre du projet LIVRAISON RIKI.

Déclencheurs de l'ÉFVP applicables (art. 3.3 Loi 25) :

- Le projet implique l'**acquisition, le développement et la refonte** d'un système d'information portant sur les renseignements personnels.
- La **communication de renseignements personnels à l'extérieur du Québec** est envisagée (hébergement actuel sur une plateforme de développement américaine).
- L'organisation utilise des **technologies permettant d'identifier, localiser ou profiler** une personne (GPS en temps réel, préférences de commande).
- Le projet implique le **traitement automatisé** de renseignements personnels (profilage pour recommandations, tarification dynamique).

2. Description détaillée du projet

LIVRAISON RIKI est une plateforme de livraison alimentaire locale pour la région de Rimouski. Elle met en relation des **clients particuliers**, des **restaurants partenaires** et des **livreurs indépendants** via une application mobile (iOS, Android) et une interface web. Le service inclut la prise de commande, le paiement électronique, le suivi GPS en temps réel, la facturation conforme **MEV-WEB (Revenu Québec)** et un service de clavardage.

2.1 Parties prenantes

Responsable du traitement	LIVRAISON RIKI (entreprise en constitution) 131 rue des Flandres, Rimouski (Québec) G5M 0L3, Canada
Responsable Loi 25	**Yasser MAKHLOUF** Courriel : confidentialite@livraisonriki.com Tél. : 1-418-509-2069
Sous-traitants principaux	Stripe (paiements · USA/Canada) · Resend (courriels · USA) · OVH (hébergement cible · Québec) · Firebase (notifications · USA)
Types d'utilisateurs	Clients, restaurants partenaires, livreurs, administrateurs

3. Inventaire des renseignements personnels (RP)

Catégorie	Données collectées	Finalité	Base légale
Identité	Nom, prénom, date de naissance	Création compte, vérification âge pour certaines commandes	Consentement + exécution contrat
Contact	Courriel, téléphone, adresse postale	Communication, livraison, support client	Exécution du contrat
Localisation	Position GPS en temps réel	Attribution livreur, suivi commande, calcul distance	Consentement explicite
Transactions	Historique commandes, montants, pourboires	Facturation, comptabilité, programme fidélité	Exécution contrat + obligations fiscales
Paiement	Token Stripe (jamais le numéro carte complet)	Paiement sécurisé	Exécution du contrat
Préférences	Restaurants favoris, allergies déclarées, langue	Personnalisation, pertinence du service	Consentement
Techniques	Jetons push, logs d'accès, IP, user-agent	Sécurité, prévention fraude, diagnostic	Intérêt légitime
Communications	Messages chat client-livreur-restaurant, tickets support	Service, résolution de litiges	Exécution contrat
Documents fiscaux	Factures MEV-WEB (hash cryptographique inclus)	Conformité Revenu Québec	Obligation légale

Note : Aucun RP de catégorie sensible au sens de l'article 59 de la Loi n'est systématiquement collecté (données de santé, origine ethnique, orientation sexuelle, opinions politiques, données biométriques). Les allergies alimentaires éventuellement déclarées par l'utilisateur dans son profil sont facultatives et traitées avec les mesures de sécurité renforcées de la section 7.

4. Flux de données et sous-traitants

4.1 Transferts hors Québec (art. 17 Loi 25)

Conformément à l'**article 17 de la Loi 25**, toute communication de RP à l'extérieur du Québec requiert une évaluation préalable. Les flux identifiés et leurs mesures de mitigation sont les suivants :

Fournisseur	Juridiction	RP transmis	Mesure contractuelle / technique
Stripe Inc.	Irlande / USA	Nom, courriel, montant, token carte	DPA signé · Chiffrement TLS 1.3 · PCI-DSS niveau 1
Resend (envoi courriels)	USA	Nom, courriel, contenu courriel	DPA signé · Chiffrement en transit · Suppression 30 j
Firebase Cloud Messaging	USA	Jeton push anonyme (pas d'identité)	Aucun RP direct · Jeton rotatif · DPA Google
Hébergement cible OVH	Québec (Beauharnois)	Ensemble des RP	**Pas de transfert hors QC ✓**
Google / Apple Maps	USA	Coordonnées de livraison (anonymisées)	Appels transitoires · pas de stockage côté fournisseur

4.2 Évaluation du niveau de protection équivalent

L'ÉFVP conclut que les juridictions concernées (USA · Irlande) offrent un niveau de protection **globalement comparable** à celui du Québec, sous réserve de l'application de clauses contractuelles conformes au modèle recommandé par la Commission d'accès à l'information (CAI). Tous les sous-traitants hors QC sont liés par un contrat de traitement (DPA) comportant minimalement :

- Les finalités précises et limitées du traitement
- L'interdiction de traitement ultérieur sans autorisation
- Les mesures de sécurité (chiffrement, pseudonymisation, contrôle d'accès)
- Les délais de conservation et destruction
- La notification des incidents dans un délai raisonnable (≤ 72 h)
- La restitution ou destruction des données à la fin du contrat
- Le droit d'audit annuel sur les mesures techniques et organisationnelles

5. Finalités du traitement (art. 8.1 Loi 25)

Les RP collectés par LIVRAISON RIKI servent exclusivement aux finalités suivantes, préalablement et clairement communiquées à l'utilisateur lors de son inscription (article 8 de la Loi) :

Prestation du service de commande et livraison	**Exécution du contrat**
Facturation et conformité fiscale (TPS, TVQ, MEV-WEB)	**Obligation légale**
Communication opérationnelle (confirmations, suivi, support)	**Exécution du contrat**
Prévention de la fraude et sécurité du service	**Intérêt légitime**
Personnalisation (recommandations, programme de fidélité)	**Consentement**
Analyses statistiques agrégées et anonymisées	**Intérêt légitime**
Communications marketing (facultatif, désactivable)	**Consentement explicite**

6. Durées de conservation (art. 23 Loi 25)

Catégorie	Durée	Fondement
Compte client actif	Tant que le compte est actif	Nécessité contractuelle
Compte inactif	Suppression / anonymisation après 24 mois d'inactivité	Art. 23 Loi 25 — nécessité
Historique commandes	6 ans après dernière commande	Obligations comptables + MEV-WEB
Factures MEV-WEB	6 ans minimum (immuable)	Loi fiscale QC + fédérale
Logs de sécurité	24 mois	Intérêt légitime (sécurité)
Communications support	36 mois	Résolution de litiges
Localisation GPS temps réel	Supprimée immédiatement après la livraison	Minimisation (art. 10)
Jetons push	90 jours après dernière utilisation	Pertinence technique

7. Analyse des risques et mesures d'atténuation

Les risques identifiés sont évalués selon leur **probabilité** (de 1 à 5) et leur **impact** sur les droits des personnes concernées (de 1 à 5). Les mesures d'atténuation ramènent chaque risque à un niveau **résiduel** ≤ **2**, considéré comme **acceptable**.

Risque	P × I initial	Mesures techniques et organisationnelles	P × I résiduel
Fuite de la base de données	4 × 5 = 20	Chiffrement AES-256 au repos · TLS 1.3 en transit · MongoDB avec authentification forte · Backups chiffrés GPG offsite · Accès admin par VPN uniquement	1 × 3 = 3
Accès non autorisé à un compte	3 × 4 = 12	Mots de passe bcrypt + salt · 2FA facultatif · Rate limiting login · Lockout après 5 tentatives · Session JWT courte (24h) · Révocation push possible	1 × 2 = 2
Interception trafic réseau	2 × 4 = 8	TLS 1.3 obligatoire · HSTS préchargé · Certificate pinning dans l'app · Pas de HTTP en clair	1 × 2 = 2
Détournement de données GPS	3 × 5 = 15	GPS supprimé immédiatement post-livraison · Granularité réduite au niveau quartier dans l'historique · Pas de corrélation inter-courses	1 × 2 = 2
Profilage non consenti	3 × 4 = 12	Consentement granulaire · Opt-out marketing en 1 clic · Pas de revente à des tiers · Pas de courtage de données	1 × 1 = 1
Fraude paiement	3 × 4 = 12	Stripe PCI-DSS niveau 1 · 3D-Secure obligatoire · Détection fraude Stripe Radar · Jamais de carte en clair chez nous	1 × 2 = 2
Erreur sous-traitant hors QC	3 × 3 = 9	DPA signés · Clauses de notification 72h · Audit annuel · Préférence pour fournisseurs CA/QC	1 × 2 = 2
Perte de disponibilité du service	3 × 2 = 6	Backups quotidiens · Monitoring 24/7 · Snapshots VPS · Procédure de restauration documentée · RTO : 4h · RPO : 24h	1 × 1 = 1

8. Exercice des droits (art. 27-30 Loi 25)

LIVRAISON RIKI garantit à toute personne concernée l'exercice effectif des droits suivants, avec une réponse formelle dans un délai maximal de **30 jours calendaires** suivant la réception de la demande :

Droit d'accès (art. 27)

Obtenir une copie structurée de l'ensemble des RP détenus (format JSON ou PDF au choix).

Droit de rectification (art. 28)

Correction immédiate des RP inexacts, incomplets ou équivoques.

Droit à l'effacement (art. 28.1)

Suppression définitive sauf obligation légale de conservation (ex. factures 6 ans).

Droit à la portabilité (art. 27)

Transmission des RP vers un autre fournisseur dans un format technologique couramment utilisé.

Droit d'opposition au profilage automatisé (art. 12.1)

Retrait du consentement et désactivation des recommandations/tarification personnalisée.

Droit de retrait du consentement (art. 14)

Désactivation en un clic depuis les paramètres du compte.

Droit de plainte à la CAI

Dépôt d'une plainte auprès de la Commission d'accès à l'information du Québec sans conditions préalables.

Procédure interne : toute demande est reçue à l'adresse confidentialite@livraisonriki.com. Le Responsable Loi 25 enregistre la demande dans un registre dédié, confirme la réception sous 48 h et répond au fond dans les 30 jours. En cas de refus, les motifs sont écrits et le recours à la CAI est systématiquement indiqué.

9. Gestion des incidents de confidentialité (art. 3.5 + 28.1)

En cas d'incident de confidentialité (accès non autorisé, utilisation à des fins non prévues, communication non autorisée ou perte de RP), la procédure suivante s'applique :

1. **T + 0 h** — Détection par le monitoring automatisé ou signalement humain.
2. **T + 1 h** — Confinement : révocation d'accès, isolation du système touché, rotation des secrets concernés.
3. **T + 24 h** — Évaluation du risque de préjudice sérieux (RPS) par le Responsable Loi 25.
4. **T + 72 h max** — Si RPS confirmé : notification formelle à la **Commission d'accès à l'information (CAI)** et aux personnes concernées (courriel + push).
5. **T + 30 j** — Rapport post-incident détaillé consigné au **registre des incidents de confidentialité** (obligatoire, art. 3.8).
6. **Rétrospective** — Mise à jour des mesures techniques, formation équipe, test de la procédure.

10. Approbation et révision

La présente ÉFVP est approuvée par le Responsable Loi 25 de LIVRAISON RIKI. Elle fait l'objet d'une révision **annuelle obligatoire** et d'une révision ponctuelle à chaque changement significatif (nouveau sous-traitant, nouvelle finalité, incident majeur, modification législative).

Responsable Loi 25

Yasser MAKHLOUF

_____

Signature · Date

Direction LIVRAISON RIKI (entreprise en constitution)

Yasser MAKHLOUF

_____

Signature · Date

Historique des révisions

Version	Date	Modifications	Auteur
1.0	6 octobre 2026	Création initiale (migration prévue vers OVH Beauharnois)	Yasser MAKHLOUF