LIVRAISON RIKI

Privacy Impact Assessment (PIA)

LIVRAISON RIKI Project — Local Delivery Platform

Document: **PIA · Québec Law 25, Section 3.3**
Version 1.1 · Prepared on November 7, 2026
Questions about Law 25: **confidentialite@livraisonriki.com**

LIVRAISON RIKI (business in the process of being incorporated)
25 rue Saint-Germain Est - Floor 1, Rimouski (Québec) G5L 1A3, Canada
confidentialite@livraisonriki.com
livraisonriki.com

1. Preamble and Legal Context

This Privacy Impact Assessment (PIA) is carried out in accordance with **section 3.3 of the Act respecting the protection of personal information in the private sector** (CQLR, c. P-39.1), as amended by the **Act to modernize legislative provisions as regards the protection of personal information** (hereinafter "Law 25"). Its purpose is to identify, assess and mitigate the privacy risks to the individuals concerned in the context of the LIVRAISON RIKI project.

Applicable PIA triggers (s. 3.3, Law 25):

- The project involves the **acquisition, development and overhaul** of an information system involving personal information.
- The **communication of personal information outside Québec** is contemplated (current hosting on a U.S. development platform).
- The organization uses **technologies that make it possible to identify, locate or profile** an individual (real-time GPS, order preferences).
- The project involves the **automated processing** of personal information (profiling for recommendations, dynamic pricing).

2. Detailed Project Description

LIVRAISON RIKI is a local food delivery platform for the Rimouski region. It connects **individual customers**, **partner restaurants** and **independent couriers** through a mobile application (iOS, Android) and a web interface. The service includes order placement, electronic payment, real-time GPS tracking, invoicing compliant with **MEV-WEB (Revenu Québec)** and a chat service.

2.1 Stakeholders

Data Controller	LIVRAISON RIKI (business in the process of being incorporated) 25 rue Saint-Germain Est - Floor 1, Rimouski (Québec) G5L 1A3, Canada
Person in Charge of the Protection of Personal Information (Law 25)	Email: confidentialite@livraisonriki.com
Main Service Providers	Stripe (payments · USA/Canada) · Resend (emails · USA) · OVH (target hosting · Québec) · Firebase (notifications · USA)
User Types	Customers, partner restaurants, couriers, administrators

3. Inventory of Personal Information (PI)

Category	Data Collected	Purpose	Legal Basis
Identity	Last name, first name, date of birth	Account creation, age verification for certain orders	Consent + performance of contract
Contact	Email, telephone, mailing address	Communication, delivery, customer service	Performance of contract
Location	Real-time GPS position	Driver assignment, order tracking, distance calculation	Explicit consent
Transactions	Order history, amounts, tips	Invoicing, accounting, loyalty program	Performance of contract + tax obligations
Payment	Stripe token (never the full card number)	Secure payment	Performance of contract
Preferences	Favourite restaurants, declared allergies, language	Personalization, relevance of the service	Consent
Technical	Push tokens, access logs, IP address, user-agent	Security, fraud prevention, diagnostics	Legitimate interest
Communications	Customer-driver-restaurant chat messages, customer service requests	Service, dispute resolution	Performance of contract
Tax documents	MEV-WEB invoices (cryptographic hash included)	Revenu Québec compliance	Legal obligation

Note: No PI belonging to a sensitive category within the meaning of section 59 of the Act is systematically collected (health data, ethnic origin, sexual orientation, political opinions, biometric data). Any food allergies declared by the user in their profile are optional and are processed with the enhanced security measures described in section 7.

4. Data flows and subcontractors

4.1 Transfers outside Québec (s. 17 Law 25)

In accordance with **section 17 of Law 25**, any communication of PI outside Québec requires a prior assessment. The identified flows and their mitigation measures are as follows:

Provider	Jurisdiction	PI transmitted	Contractual / technical measure
Stripe Inc.	Ireland / USA	Name, email, amount, card token	Signed DPA · TLS 1.3 encryption · PCI-DSS Level 1
Resend (email delivery)	USA	Name, email, email content	Signed DPA · Encryption in transit · 30-day deletion
Firebase Cloud Messaging	USA	Anonymous push token (no identity)	No direct PI · Rotating token · Google DPA
OVH target hosting	Québec (Beauharnois)	All PI	**No transfer outside QC ✓**
Google / Apple Maps	USA	Delivery coordinates (anonymized)	Transient calls · no storage on the provider's side

4.2 Assessment of the equivalent level of protection

The PIA concludes that the jurisdictions concerned (USA · Ireland) offer a level of protection that is **broadly comparable** to that of Québec, subject to the application of contractual clauses consistent with the model recommended by the Commission d'accès à l'information du Québec (CAI). All subcontractors outside QC are bound by a data processing agreement (DPA) containing, at a minimum:

- The specific and limited purposes of the processing
- The prohibition of further processing without authorization
- Security measures (encryption, pseudonymization, access control)
- Retention and destruction periods
- Notification of incidents within a reasonable time (≤ 72 h)
- The return or destruction of data at the end of the contract
- The right to conduct an annual audit of technical and organizational measures

5. Purposes of the Processing (s. 8.1, Law 25)

The personal information (PI) collected by LIVRAISON RIKI is used exclusively for the following purposes, which are clearly communicated to the user in advance at registration (section 8 of the Act):

Provision of the ordering and delivery service	**Performance of the contract**
Invoicing and tax compliance (GST, QST, MEV-WEB)	**Legal obligation**
Operational communications (confirmations, tracking, customer service)	**Performance of the contract**
Fraud prevention and service security	**Legitimate interest**
Personalization (recommendations, loyalty program)	**Consent**
Aggregated and anonymized statistical analyses	**Legitimate interest**
Promotional communications (optional, can be disabled)	**Express consent**

6. Retention Periods (s. 23, Law 25)

Category	Period	Basis
Active customer account	As long as the account is active	Contractual necessity
Inactive account	Deletion / anonymization after 24 months of inactivity	Sec. 23, Law 25 — necessity
Order history	6 years after the last order	Accounting obligations + MEV-WEB
MEV-WEB invoices	6 years minimum (immutable)	Québec and federal tax legislation
Security logs	24 months	Legitimate interest (security)
Customer service communications	36 months	Dispute resolution
Real-time GPS location	Deleted immediately after delivery	Minimization (sec. 10)
Push tokens	90 days after last use	Technical relevance
Dish searches (with consent)	1, 3, 6 months or 1 year at the customer's choice; consent requested again at the end of the period, failing which the data is erased	Consent (sec. 12)

7. Risk Analysis and Mitigation Measures

The identified risks are assessed according to their **likelihood** (from 1 to 5) and their **impact** on the rights of the individuals concerned (from 1 to 5). The mitigation measures bring each risk down to a **residual level** ≤ **2**, which is considered **acceptable**.

Risk	Initial L × I	Technical and organizational measures	Residual L × I
Database breach	4 × 5 = 20	AES-256 encryption at rest · TLS 1.3 in transit · MongoDB with strong authentication · Encrypted GPG offsite backups · Admin access via VPN only	1 × 3 = 3
Unauthorized access to an account	3 × 4 = 12	Passwords hashed with bcrypt + salt · Optional 2FA · Login rate limiting · Lockout after 8 attempts within 15 minutes · Short-lived JWT session (24h) · Push revocation possible	1 × 2 = 2
Network traffic interception	2 × 4 = 8	TLS 1.3 mandatory · Preloaded HSTS · Certificate pinning in the application · No plaintext HTTP	1 × 2 = 2
Misappropriation of GPS data	3 × 5 = 15	GPS data deleted immediately after delivery · Granularity reduced to neighbourhood level in history · No correlation across trips	1 × 2 = 2
Profiling without consent	3 × 4 = 12	Granular consent · One-click unsubscribe from promotional communications · No resale to third parties · No data brokerage	1 × 1 = 1
Payment fraud	3 × 4 = 12	Stripe PCI-DSS Level 1 · 3D Secure mandatory · Stripe Radar fraud detection · Card details never held in clear text on our systems	1 × 2 = 2
Subcontractor error outside Québec	3 × 3 = 9	Signed DPAs · 72-hour notification clauses · Annual audit · Preference for Canadian/Québec suppliers	1 × 2 = 2
Loss of service availability	3 × 2 = 6	Daily backups · 24/7 monitoring · VPS snapshots · Documented restoration procedure · RTO: 4h · RPO: 24h	1 × 1 = 1

8. Exercise of rights (ss. 27-30, Law 25)

LIVRAISON RIKI guarantees to every individual concerned the effective exercise of the following rights, with a formal response within a maximum of **30 calendar days** of receipt of the request:

Right of access (s. 27)

Obtain a structured copy of all personal information held (JSON or PDF format, at the person's choice).

Right of rectification (s. 28)

Immediate correction of inaccurate, incomplete or equivocal personal information.

Right to erasure (s. 28.1)

Permanent deletion, unless a legal retention obligation applies (e.g., invoices, 6 years).

Right to portability (s. 27)

Transmission of PI to another provider in a commonly used technological format.

Right to object to automated profiling (s. 12.1)

Withdrawal of consent and deactivation of personalized recommendations and pricing.

Right to withdraw consent (s. 14)

One-click deactivation from the account settings.

Right to file a complaint with the CAI

Filing of a complaint with the Commission d'accès à l'information du Québec (CAI) without any preconditions.

Internal procedure: all requests are received at confidentialite@livraisonriki.com. The Person in Charge of Law 25 records the request in a dedicated register, acknowledges receipt within 48 h and responds on the merits within 30 days. In the event of a refusal, the reasons are provided in writing and the right of recourse to the CAI is systematically indicated.

9. Confidentiality Incident Management (s. 3.5 + 28.1)

In the event of a confidentiality incident (unauthorized access, use for unintended purposes, unauthorized communication or loss of PI), the following procedure applies:

1. **T + 0 h** — Detection through automated monitoring or human report.
2. **T + 1 h** — Containment: revocation of access, isolation of the affected system, rotation of the relevant secrets.
3. **T + 24 h** — Assessment of the risk of serious injury (RSI) by the Person in Charge of Law 25.
4. **T + 72 h max** — If RSI is confirmed: formal notification to the **Commission d'accès à l'information (CAI)** and to the individuals concerned (email + push notification).
5. **T + 30 d** — Detailed post-incident report recorded in the **confidentiality incident register** (mandatory, s. 3.8).
6. **Retrospective** — Update of technical measures, team training, testing of the procedure.

10. Approval and Review

This PIA is approved by the Person in Charge of Law 25 of LIVRAISON RIKI. It is subject to a **mandatory annual review** and to an ad hoc review upon any significant change (new service provider, new purpose, major incident, legislative amendment).

Person in Charge of Law 25

_____

Signature · Date

LIVRAISON RIKI Management (company in the process of incorporation)

_____

Signature · Date

Revision History

Version	Date	Changes	Author
1.0	October 6, 2026	Initial creation (migration to OVH Beauharnois planned)	LIVRAISON RIKI Management