Évaluation des Facteurs relatifs à la Vie Privée

Hébergement infonuagique OVH Canada — Beauharnois (Québec)

Organisation responsable	Nathan Dufresne
Nom d'entreprise	Petit gros répare gros
Forme juridique	Entreprise individuelle (Québec)
NEQ	2281239287
Adresse	3370 rue des Prairies, Trois-Rivières (Québec) G8V 1W6, Canada
Courriel	support@gestionpro360.ca
Document version	1.0 — post-migration Contabo → OVH Canada
Date de publication	21 avril 2026
Conformité visée	Loi 25 — RLRQ c P-39.1

Document consultable publiquement à https://www.gestionpro360.ca/docs/EFVP-OVH.pdf

1. Contexte et objectifs

1.1 Présentation de GestionPro 360

GestionPro 360 est une plateforme logicielle infonuagique (SaaS) de gestion d'entreprise destinée aux petites et moyennes entreprises (PME) québécoises. La plateforme couvre : relation client, pipeline commercial, devis et facturation conforme TPS/TVQ, paiements, caisse POS, catalogue et inventaire, gestion fournisseurs, projets et tâches, suivi du temps, ressources humaines, comptabilité, marketing, rapports et portails client.

L'architecture est **multi-locataire par isolation complète** : chaque client dispose d'un conteneur applicatif dédié, d'une base de données Postgres privée, de son propre cache Redis, et d'un sous-domaine unique {slug}.gestionpro360.ca. Les données d'un client ne peuvent jamais être accédées par un autre client.

1.2 Changement de contexte d'hébergement (avril 2026)

Jusqu'au 20 avril 2026, l'infrastructure GestionPro 360 était hébergée chez **Contabo GmbH** dans leur centre de données situé à St. Louis (Missouri, États-Unis). Cette configuration impliquait un transfert transfrontière des données couverts par les articles 17 et 18 de la Loi 25.

Le 20 avril 2026, l'intégralité du stack a été migrée vers **OVH Hébergement Inc.**, centre de données de Beauharnois (Québec, Canada). **Les données demeurent désormais intégralement sur le territoire québécois et canadien.** La migration a été effectuée sans perte de données et sans interruption de service visible par les abonnés.

1.3 Objectifs de la présente évaluation

La présente évaluation des facteurs relatifs à la vie privée (EFVP) a pour objectifs :

- Documenter les caractéristiques du nouveau contexte d'hébergement OVH Canada
- Identifier les catégories de renseignements personnels traités et leur finalité
- Évaluer les risques résiduels et les mesures d'atténuation mises en place
- Démontrer la conformité aux obligations de la Loi 25 (articles 3.1, 8, 17, 18, 28)
- Tenir à disposition des personnes concernées et des autorités un document de référence

2. Nature des données traitées

GestionPro 360 traite deux catégories principales de personnes concernées : (a) les **utilisateurs directs** de la plateforme (administrateurs tenant, employés invités par le tenant) ; (b) les **clients finaux des tenants** dont les tenants gèrent la relation d'affaires via la plateforme.

2.1 Utilisateurs directs (admins tenant + employés invités)

- Identification : nom, prénom, adresse courriel, numéro de téléphone
- Rôle et permissions : rôle applicatif (admin, comptable, vendeur, RH, etc.)
- Authentification : mot de passe (hash bcrypt), jeton JWT HS256, support TOTP disponible (colonne totp_secret dans le registre administrateur)
- Journaux d'activité : date et heure de connexion, adresse IP, user agent (table admin_audit_log)

2.2 Clients finaux des tenants (contacts B2B)

- Identification : nom d'entreprise, personne-contact, adresse courriel, numéro de téléphone
- Coordonnées postales : adresse de facturation, adresse de livraison
- Identification fiscale : NEQ, numéros TPS/TVQ lorsque fournis par le tenant
- Historique commercial : devis, factures, paiements, soldes de compte

2.3 Données comptables et financières

- Transactions financières : émission et encaissement de factures, taxes TPS/TVQ
- Comptabilité : plan comptable, journal des opérations, balance, états financiers
- Paiements : références transaction Stripe (tokenisées par Stripe), dernier 4 chiffres carte (le cas échéant)
- Données RH : liste d'employés du tenant, rôles et permissions uniquement (la paie n'est pas traitée par la plateforme)

2.4 Analytique d'usage

Les statistiques d'utilisation de la plateforme sont collectées via une instance **Plausible Analytics auto-hébergée** (ne transmet aucune donnée à un tiers). Plausible n'utilise pas de cookies traçants et respecte les préférences *Do Not Track* par défaut.

3. Finalités et bases légales du traitement

Finalité	Base légale / justification
Fourniture du service contractuel	Exécution du contrat avec l'abonné tenant (art. 8 Loi 25, « nécessaire à l'exécution d'un contr
Facturation et conformité fiscale	Émission des factures de l'abonnement, déclaration TPS/TVQ. Base : obligation légale (Loi s
Sécurité et intégrité de la plateforme	Journal d'audit des actions administratives, détection d'anomalies, enquête après incident. Ba
Support technique	Réponse aux demandes de support par courriel. Les tickets peuvent contenir des extraits de
Analytique d'usage anonymisée	Amélioration produit via Plausible (sans cookies traçants). Base : intérêt légitime + consenter

Les données ne sont jamais revendues à des tiers, ni utilisées pour du profilage publicitaire, ni transmises à un prestataire extérieur hors des fournisseurs techniques strictement nécessaires (OVH, Stripe, Brevo, Backblaze).

4. Lieu de traitement et de stockage (section centrale)

4.1 Hébergeur principal — OVH Canada

Raison sociale	OVH Hébergement Inc. (filiale canadienne du groupe OVHcloud)
Adresse enregistrée	8250 rue Boulet, Beauharnois (Québec) J6N 0E7, Canada
Centre de données	BHS (Beauharnois, Québec)
Type d'infrastructure	Serveur privé virtuel (VPS) dédié, locataire unique
Spécifications	8 vCores, 24 GB RAM, 200 GB SSD NVMe, bande passante illimitée
Certifications OVH	ISO 27001, SOC 2, NIST (voir ovhcloud.com pour liste exhaustive)
Adresse IPv4 publique	54.39.98.101
Nom d'hôte	vps-54f2f412.vps.ovh.ca

4.2 Sauvegardes — localisation

Les sauvegardes quotidiennes sont redondées sur **trois niveaux**, **toutes situées au Canada** :

• **Niveau 1 — Locale sur serveur OVH** : /opt/gp360/backups/, pg_dump quotidien du hub et de chaque base de données tenant. Rotation à 7 jours. Localisation : Beauharnois, Québec.

• **Niveau 2 — Snapshot quotidien OVH** : sauvegarde image complète du VPS fournie par OVH, conservée sur l'infrastructure OVH Canada. Rétention selon offre OVH. Localisation : Beauharnois, Québec.

• **Niveau 3 — Off-site chiffré chez Backblaze B2** : copie quotidienne des dumps de base de données et des configurations, région **ca-east-006** (Backblaze Canada East, Toronto, Ontario). Rotation automatique à 30 jours. **Jamais stockées hors du Canada.**

Conclusion sur la localisation : aucun transfert transfrontière de données personnelles n'intervient dans l'exploitation normale de la plateforme. Les articles 17 et 18 de la Loi 25 relatifs à la communication hors Québec ne s'appliquent donc pas au traitement courant.

4.3 Sous-traitants opérationnels (traitement de données)

Sous-traitant	Rôle	Localisation	Données traitées
OVH Hébergement Inc.	Hébergement infrastructure	Beauharnois, Québec, Canada	Toutes données applicatives
Backblaze Inc.	Sauvegarde off-site chiffrée	Toronto, Ontario, Canada (ca-east-006)	Dumps DB + configs (AES-256)

Stripe Payments Canada	Traitement des paiements d'abonnement	Toronto, Canada	Transactions, tokens de carte (pas de PAN)
Brevo SAS	Expédition courriels transactionnels	Paris, France (UE)	Adresse courriel + contenu courriel
Let's Encrypt (ISRG)	Certificats TLS	International (Internet)	Aucune donnée personnelle (validation par DNS)

Note Brevo (hors Canada) : Brevo est utilisé uniquement pour l'expédition de courriels transactionnels (factures d'abonnement, mot de passe oublié, alertes). Les adresses courriel transitent par Brevo mais ne sont pas stockées de façon persistante à des fins de marketing. Un accord de traitement conforme RGPD (équivalent Loi 25) est en vigueur avec Brevo.

5. Durée de conservation

Les durées de conservation sont alignées sur les obligations fiscales québécoises et fédérales, ainsi que sur les intérêts légitimes de sécurité.

Catégorie de données	Durée de conservation	Fondement
Données applicatives actives (tenant)	Durée du contrat SaaS	Exécution du contrat
Données applicatives après résiliation	30 jours (grace period récupération client), puis suppression	Droit à la portabilité — Loi 25 art. 28
Sauvegardes off-site B2	30 jours (rotation automatique)	Disaster recovery
Journaux d'audit administrateur	24 mois	Sécurité + enquête éventuelle
Factures + pièces comptables	6 ans fiscaux	Obligation ARC + Revenu Québec
Courriels de support	24 mois après clôture du ticket	Historique service client
Analytique Plausible	Agrégée, sans identifiant individuel, 12 mois	Intérêt légitime
Cookies (consentement + préférences)	13 mois	Loi 25 + CNIL convergence

6. Mesures de sécurité techniques et organisationnelles

6.1 Chiffrement

• **En transit :** TLS 1.2+ (négocié à 1.3 pour les clients modernes). Certificat wildcard *.gestionpro360.ca délivré par Let's Encrypt (E8), renouvellement automatique via ACME DNS-01. HSTS activé avec max-age 1 an.

• **Au repos — bases de données :** PostgreSQL 16, chiffrement du volume Docker au niveau disque (AES-256 via LUKS au niveau hôte sur OVH).

• **Au repos — sauvegardes off-site :** chiffrement AES-256 côté Backblaze (server-side encryption) + clés applicatives gérées par Nathan Dufresne.

• **Secrets applicatifs :** extraits des fichiers docker-compose vers fichiers .env dédiés avec permissions chmod 600 root:root (non lisibles par processus non-privilégiés). Clés Stripe Live, secrets webhook, clés JWT, mots de passe DB stockés ainsi.

6.2 Isolation entre locataires

Chaque tenant dispose de :

• Un conteneur applicatif Docker dédié (aucune colocation mémoire ni CPU partagée)

• Une base de données PostgreSQL propre (process et volume distincts)

• Une instance Redis propre (cache et broker Celery séparés)

• Un sous-domaine unique et un réseau Docker interne privé (gp360-{slug}_internal)

• Des secrets applicatifs propres (SECRET_KEY JWT, mot de passe DB, mot de passe admin)

6.3 Contrôle d'accès

• **Accès serveur (SSH) :** clé Ed25519 uniquement, authentification par mot de passe désactivée. Un seul utilisateur autorisé (Nathan Dufresne).

• **Authentification applicative :** mot de passe bcrypt + jeton JWT HS256. Expiration jeton : 8 heures (480 minutes).

• **Authentification à deux facteurs :** support TOTP implémenté au niveau du schéma (colonne totp_secret dans admin_users), activation à la discrétion de l'administrateur.

• **Registre d'accès :** table admin_audit_log enregistrant pour chaque action administrative : courriel, type d'action, tenant ciblé, détails JSON, adresse IP, user agent, horodatage UTC.

6.4 Exposition réseau

Le serveur OVH expose **uniquement 3 ports externes** : 22 (SSH, restreint par clé), 80 (HTTP, redirige en 301 vers HTTPS), 443 (HTTPS). Tous les autres services (bases de données, Redis, conteneurs applicatifs

internes) sont isolés par les réseaux Docker privés et ne sont jamais exposés à l'Internet. Le reverse proxy Caddy termine les connexions TLS et route vers les conteneurs internes via leur nom DNS Docker.

7. Droits des personnes concernées (Loi 25)

Les personnes concernées (abonnés, utilisateurs invités, clients finaux des tenants) disposent des droits suivants, qui peuvent être exercés en écrivant à support@gestionpro360.ca :

Droit	Modalité d'exercice	Délai de réponse
Droit d'accès (art. 27)	Consultation directe dans le panneau admin du tenant OU demande écrite	30 jours maximum
Droit de rectification (art. 28)	Modification directe dans l'application OU demande écrite	30 jours maximum
Droit d'effacement (art. 28.1)	Export préalable disponible au format <code>.gp360bak</code> (JSON chiffré compressé chiffré). Suppr	72 heures ouvrables
Droit à la portabilité (art. 27 al. 3)	Export automatisé au format <code>.gp360bak</code> + exports CSV/Excel par module	7 jours
Droit d'opposition	Bannière cookies (refus du suivi analytique). Communications marketing par opt-out explicite.	Immédiat
Droit de déposer plainte	Commission d'accès à l'information du Québec (CAI), www.cai.gouv.qc.ca	N/A

7.1 Personne-responsable désignée

Conformément à l'article 3.1 de la Loi 25, la personne responsable de la protection des renseignements personnels est :

Nathan Dufresne
Petit gros répare gros · NEQ 2281239287
3370 rue des Prairies, Trois-Rivières (Québec) G8V 1W6
Courriel : support@gestionpro360.ca

8. Évaluation des risques et mesures d'atténuation

Analyse des principaux risques résiduels identifiés après mise en œuvre des mesures de sécurité décrites en section 6 :

Risque identifié	Prob.	Impact	Mesures d'atténuation
Panne majeure du datacenter OVH Beauharnois	Très faible	Critique	Sauvegardes redondantes (locale + OVH snapshot + Backblaze ca-east-0
Compromission du compte administrateur de la plateforme	Faible	Élevé	Authentification par clé SSH Ed25519 uniquement. Journal d'audit complet
Tentative d'accès transversal entre tenants (escalade)	Très faible	Critique	Isolation physique par conteneurs Docker distincts. Secrets applicatifs prop
Fuite accidentelle de secrets dans les logs	Moyenne	Moyen	Secrets stockés dans <code>.env</code> <code>chmod 600</code>. App
Perte de données suite à incident opérationnel	Faible	Élevé	Sauvegardes automatiques quotidiennes redondées. Rotation 30 jours B2,
Demande abusive d'accès par un tiers non autorisé	Faible	Élevé	Vérification systématique de l'identité du demandeur (courriel de contact de

9. Conclusion et révision

9.1 Évaluation globale de conformité

Suite à la migration du 20 avril 2026, la plateforme GestionPro 360 exploitée par Nathan Dufresne (Petit gros répare gros) présente un niveau de conformité à la Loi 25 évalué comme **satisfaisant** pour les raisons suivantes :

- **Localisation québécoise et canadienne des données** — élimination des transferts transfrontières, conformité renforcée aux articles 17 et 18.
- **Personne-responsable désignée** conformément à l'article 3.1, joignable à support@gestionpro360.ca.
- **Durées de conservation documentées et alignées** sur les obligations fiscales et les intérêts légitimes.
- **Procédures d'exercice des droits** opérationnelles, avec délais explicites (72 heures pour la suppression).
- **Mesures de sécurité techniques** conformes aux bonnes pratiques de l'industrie (chiffrement, isolation, audit).

9.2 Points d'amélioration identifiés (roadmap interne)

- Activation effective du TOTP pour le compte administrateur principal
- Mise en place d'un pare-feu applicatif (rate limiting, WAF) sur les endpoints sensibles
- Rotation planifiée des credentials B2, FTP et clés Stripe dans les 7 jours suivant la migration
- Rédaction d'un plan de continuité d'activité (PCA) formalisé
- Nomination d'un délégué à la protection des données externe si le nombre d'abonnés dépasse 25 entreprises

9.3 Révision du document

La présente évaluation sera révisée dans les cas suivants :

- Incorporation de GestionPro360 inc. (changement d'éditeur)
- Changement d'hébergeur principal ou de région de stockage
- Ajout d'un nouveau sous-traitant traitant des renseignements personnels
- Mise à jour majeure de la Loi 25 ou du RGPD (convergence européenne)
- Révision périodique d'office à échéance de 12 mois (prochaine révision : 21 avril 2027 au plus tard)

Document produit le 21 avril 2026
Responsable : Nathan Dufresne
Version : 1.0
Prochaine révision planifiée : 21 avril 2027 (ou à l'incorporation de GestionPro360 inc., premier événement

atteint)

Ce document est publié à l'adresse https://www.gestionpro360.ca/docs/EFVP-OVH.pdf et disponible pour consultation par les abonnés, les clients finaux des abonnés et les autorités compétentes (notamment la Commission d'accès à l'information du Québec).