H2Ops Privacy Policy

Last updated: October 23, 2025

---

1) Who we are and scope

H2Ops ("Horizon 2 Operations," "H2Ops," "we," "our," "us") operates **horizon2operations.com** and provides B2B services including websites, CRM implementations, process automations, and AI voice/text agents. This Privacy Policy describes how we handle Personal Information when you:

- visit or use our website and pages that link to this policy (the "Site"),
- interact with our sales, support, or marketing communications, or
- receive services as a client or prospective client (the "Services").

Roles

- For Site visitors, prospects, and our own business records, H2Ops is a **controller**.
- For client-supplied data processed in your CRM/automations/AI agents, H2Ops acts as a **processor** (or service provider) under your instructions and any applicable Data Processing Addendum (DPA).

Privacy Officer

H2Ops designates a Privacy Officer responsible for compliance with this policy and PIPEDA. Contact: **sammi@horizon2operations.com**.

---

2) Information we collect

A) You provide

- Identification and contact: name, email, phone, company, role.
- Business records: scoping notes, onboarding forms, configuration data, content you upload.
- Communications: emails, chat transcripts, support requests, call bookings.
- Billing: invoice details and transaction metadata. Card data is handled by processors; we do **not** store full card numbers.
- Marketing preferences and consent choices.

B) Collected automatically

- Usage and device data: IP address, timestamps, pages viewed, referrer, browser/OS, language, approximate location, session IDs.
- Cookies, pixels, and similar tech for analytics and site performance. We may use Google Analytics and comparable tools.

C) From third parties

- Lead and enrichment data from sales/marketing partners (e.g., Apollo) and public sources (company websites, LinkedIn, registries), in compliance with applicable laws and your preferences.

D) Service- and agent-specific data

- **Voice/SMS/telephony**: call recordings, transcriptions, and message metadata when you use AI agents or Twilio/Vapi numbers, where permitted and with required notices/consents.
- **CRM/workflow**: records you instruct us to process in Airtable, ClickUp, n8n, or similar tools.

Sensitive data We do not intentionally collect sensitive personal information. Do not submit it to us. If processing is required by a client, it must be governed by a DPA and lawful basis.

Data minimization We collect only what is necessary for stated purposes and review collection to reduce data footprint.

---

3) How we use information

- Provide, configure, and maintain the Services.
- Communicate about projects, support, security, and billing.
- Analyze performance, improve quality, and develop new features.
- Personalize content and measure campaign effectiveness.
- Detect, prevent, and investigate security incidents and abuse.
- Comply with legal obligations and enforce agreements.
- Send marketing communications where permitted; you can opt out at any time.

Automated decisioning & AI We may use AI models to route inquiries, score or prioritize leads, generate responses, and automate follow-ups. We do not make decisions with legal or similarly significant effects without human involvement. You may request human review or opt out of non-essential profiling.

---

4) Legal bases (EEA/UK where applicable)

- **Consent** (e.g., marketing, cookies, recording where required).
- **Contract** (to deliver Services you request).
- **Legitimate interests** (product improvement, security, fraud prevention, B2B outreach) balanced with your rights.
- **Legal obligation** (tax, accounting, compliance).

For Canada, processing aligns with **PIPEDA** principles of consent, limiting collection, use, disclosure, and retention.

---

5) Sharing and disclosures

We do **not** sell or rent Personal Information. We share as follows:

- **Service providers/processors** strictly for our operations, such as: Gmail/Google Workspace, n8n, Twilio, Vapi, Airtable, Apollo, Instantly, ClickUp, Bolt, Apify, web hosting/CDN, analytics, payment processors, and security tools.
- **Legal**: if required by law or to protect rights, safety, or the integrity of the Services.
- **Business transfers**: in a merger, acquisition, or asset sale, information may transfer subject to this policy.

We require processors to protect Personal Information and to process it only under our instructions. We maintain a current list of sub-processors available on request and will provide notice before adding or replacing a sub-processor where contractually required.

---

6) International transfers

We may process and store data in countries outside your own, including the United States. Where required, we rely on appropriate safeguards such as **Standard Contractual Clauses** and comparable mechanisms. Details available on request.

---

7) Retention

We keep Personal Information only as long as necessary for the purposes described or as required by law. Typical periods:

- Sales inquiries and support tickets: up to **24 months** after last interaction.
- Contracts, invoices, and tax records: **7 years**.
- Call recordings and AI agent transcripts: up to **12 months** unless you request earlier deletion or longer retention for your operations.
- Web server logs and security events: up to **12 months**. Actual retention may vary based on legal, operational, or contractual needs.

---

8) Security

We implement administrative, technical, and physical safeguards appropriate to risk, including access controls, encryption in transit, and environment hardening. No method is 100% secure. We monitor for vulnerabilities and aim to mitigate incidents promptly.

8.1) Breach notification (Canada)

We assess any breach of security safeguards. If a breach creates a **real risk of significant harm**, we will notify affected individuals and report to the Office of the Privacy Commissioner of Canada **without undue delay**, and maintain breach records for **24 months**.

---

9) Your rights and choices

Canada (PIPEDA): Access and correct your Personal Information; withdraw consent subject to legal/ contractual limits.

EEA/UK (GDPR): Request access, rectification, erasure, restriction, portability, and object to processing, including profiling based on legitimate interests or direct marketing.

California (CCPA/CPRA): Residents may request access/portability and deletion, and opt out of certain sharing for cross-context behavioral advertising. We do not sell Personal Information.

We will verify your identity before acting on requests. We aim to respond within 30 days, subject to lawful extensions. To exercise rights, email **sammi@horizon2operations.com**.

---

10) Cookies and similar technologies

We use necessary cookies for core functionality and optional cookies for analytics and performance. You can manage cookies in your browser. If we offer a cookie banner or preferences tool, your selections will be honored. Your choices persist until cleared or expired.

---

11) Communications and SMS terms

All email and SMS are sent in compliance with Canada's Anti-Spam Legislation (CASL). We record consent status and honor withdrawals promptly.

- **Email marketing**: sent under consent or lawful B2B interest. Unsubscribe any time.
- **SMS**: if you opt in, you agree to receive messages related to services, reminders, or marketing. Message frequency may vary. **Msg & data rates may apply.** Reply **STOP** to opt out and **HELP** for help. Delivery may be subject to carrier availability. We log SMS consent status as required.

---

12) Children’s privacy

Our Site and Services are for business users. We do not knowingly collect Personal Information from children under 18. If you believe a child has provided data, contact us to delete it.

13) Third-party links

The Site may contain links to third-party websites or services. Their privacy practices govern those properties. Review their policies separately.

---

14) Controller/processor addendum

For clients, a **Data Processing Addendum (DPA)** is available on request. It governs processing of your customer data, including confidentiality, sub-processors, security, and deletion/return at termination. A current list of sub-processors is available on request, and we will notify you in advance of material changes to sub-processors where contractually required.

---

15) Changes to this policy

We may update this policy to reflect changes to laws, services, or operations. We will post updates with a new "Last updated" date. Material changes may be communicated by email or prominent notice on the Site.
