noorflows — Security & Trust Questionnaire (pre-filled)

Last reviewed: 2026-07-07. For the noorflows AI support/refund agent (Shopify app) and the automations noorflows builds. Answers are honest and current — where we don't hold a certification, we say so. Questions not covered here: email syed@noorflows.com.

A public summary of our posture is at https://noorflows.com/trust. A Data Processing Agreement (DPA) is available on request.

---

1. Company & product

#	Question	Answer
1.1	What does the product do?	A governed AI customer-support + refund agent for Shopify. It answers order/return/refund questions from the merchant's real data; refunds require the merchant's one-click approval and never auto-execute.
1.2	Company size / structure	Independent, founder-run (solo). We are transparent that we are small — see §9 on certifications.
1.3	Where is it hosted?	A single dedicated server (Hetzner, EU region), Docker-based. The website is on Cloudflare.

2. Data handling

#	Question	Answer
2.1	What customer data is processed?	Shopify order, fulfillment, product, and return data needed to answer a shopper's question, plus the shopper's message. Only the scopes required: `read_customers, read_fulfillments, read_orders, read_products, read_returns, write_orders, write_returns` (least-privilege — no write access to customers, products, or content).
2.2	Is PII minimized?	Yes. Card numbers, SSNs, emails, and phone numbers are redacted to placeholders **before** the model sees them and before logging.
2.3	Data retention	Execution/history data is pruned automatically (14-day / capped-count policy). Backups follow a 14-day local / 30-day off-site retention.
2.4	Is data used to train models?	No. Merchant data is not used to train any model. LLM calls are inference-only.

3. Encryption

#	Question	Answer
3.1	Encryption in transit	TLS/HTTPS everywhere (Caddy reverse proxy). Secure, HTTP-only cookies.
3.2	Encryption at rest	Off-site backups are AES-encrypted (rclone crypt) before leaving the server. Application/automation secrets are encrypted with SOPS (age) at rest in our private repository; n8n credentials are encrypted with a pinned encryption key.
3.3	Secrets management	No plaintext secrets in version control. Secrets are SOPS/age-encrypted in a private repo and read from restricted (`0600`) files on the server; credentials can be rotated on request.

4. Access control & infrastructure

#	Question	Answer
4.1	Server access	SSH key-only — password authentication disabled, root login restricted to key (`prohibit-password`), `MaxAuthTries` limited.
4.2	Network hardening	Host firewall default-denies inbound; only 22/80/443 are open. fail2ban is active on SSH.
4.3	Webhook authenticity	Shopify webhooks are verified via HMAC-SHA256 signature against the raw body — spoofed events are rejected.
4.4	Infrastructure reproducibility	The server build is codified as an Ansible playbook (infrastructure-as-code), so configuration is documented and reproducible.

5. AI-specific safety (the core of what we do)

#	Question	Answer
5.1	Does the AI take irreversible/financial actions autonomously?	No. Refunds and returns queue for the merchant's **one-click human approval** and never execute autonomously. A database-level atomic guard prevents a refund from being executed twice.
5.2	Does it hallucinate policies?	It answers only from the merchant's real orders, products, and policies, and escalates to a human when unsure — it will not invent a policy.
5.3	Prompt-injection defense	Untrusted shopper text (emails, tickets, reviews) is treated as data, not instructions; injection patterns are detected and refused. It cannot be talked into a refund by a malicious message.
5.4	Audit trail	Every decision and action is written to an audit log the merchant controls.
5.5	AI disclosure	Customers are told they're interacting with AI (aligns with EU AI Act Art. 50 transparency).

6. Backups & disaster recovery

#	Question	Answer
6.1	Are backups taken?	Nightly automated backups of all databases + config, AES-encrypted, pushed off-site to Backblaze B2.
6.2	Are backups monitored?	Yes — a Healthchecks.io dead-man's switch alerts if a backup fails or does not run.
6.3	Has restore been tested?	**Yes.** A timed restore drill (2026-07-07) restored all databases into an isolated environment and verified integrity; measured data-restore RTO ~13 seconds.
6.4	Reliability monitoring	A self-healing monitor (with an abstain-and-escalate path), a silent-failure reconciler, a dead-letter queue, and multi-channel alerting (email/WhatsApp/Healthchecks).

7. Sub-processors

#	Sub-processor	Purpose
7.1	Shopify	Commerce platform / app host
7.2	Anthropic and/or OpenAI	LLM inference (no training on your data)
7.3	Backblaze B2	Encrypted off-site backup storage
7.4	Cloudflare	Website hosting / DNS / CDN

#	Sub-processor	Purpose
7.5	Hetzner	Server hosting (EU)
7.6	Twilio, Healthchecks.io	Operational alerting

The exact sub-processor set for a given engagement is confirmed in the DPA.

8. Data residency & privacy rights

#	Question	Answer
8.1	Data residency	Primary processing on an EU (Hetzner) server.
8.2	GDPR / CCPA	We support data-subject access/deletion rights; the app implements Shopify's `customers/data_request` and `customers/redact` compliance webhooks. DPA available on request.
8.3	Data deletion on uninstall	App uninstall triggers cleanup via the `app/uninstalled` webhook.

9. Compliance posture — what we do and don't claim

#	Question	Answer
9.1	SOC 2 / ISO 27001 / ISO 42001?	**Not currently certified.** We build to those control principles and will support your vendor review honestly, but we will never claim a certification we don't hold. If formal certification is a hard procurement requirement, tell us and we'll be straight about what we can meet today.
9.2	Incident response	We maintain a written incident-response procedure and will notify affected customers promptly of any security incident materially affecting their data.
9.3	Penetration testing	We actively study agent/LLM attack techniques (prompt injection, tool abuse) and apply OWASP LLM/agentic guidance; we do not currently hold a third-party pentest report but can discuss one for a larger engagement.

Prepared honestly. If anything here is a blocker for your procurement, email syed@noorflows.com and we'll tell you plainly what we can and cannot meet.