

# Privacy Policy

Last updated: August 21, 2025

This privacy notice for Forge Technologies Inc. ("Forge," "we," "us," or "our") describes how and why we might collect, store, use, and/or share ("process") information when you use our services ("Services"), such as when you:

- Visit [forgehq.com](https://forgehq.com) or any website of ours that links to this notice
- Use any Forge Shopify app
- Engage with our brokerage/duty drawback services and related operations

Questions or concerns? Contact [hello@forgehq.com](mailto:hello@forgehq.com).

Our role. For our Shopify app and claim-preparation services we act as a processor/service provider to the merchant (the controller/business) and process personal data only on the merchant's documented instructions (see Section 16, DPA). For brokerage/legal recordkeeping, we act as an independent controller for the copies we must retain (e.g., carrier POD/tracking and drawback filings). We are also a controller for our own B2B contact and marketing records.

---

## Summary of Key Points

- What do we collect? Business contact details you provide (merchant name, work email/phone, company, job title) and support communications. From Shopify, we sync order and inventory fields needed for U.S. duty drawback preparation. We do not retain consumer contact data from orders. For reliability, we keep a minimal webhook audit trail (topic, shop domain, time received only; no payload). For brokerage (outside the app), we obtain carrier POD and tracking data directly from carriers (e.g., FedEx/UPS/DHL).
- How do we use it? To provide and secure the Services, prepare drawback claims, comply with law, and communicate with you. No cross-site behavioral advertising.

- Do we sell/share for ads? No.
  - Cookies? We do not set non-essential cookies or pixels. The site may use strictly necessary cookies for secure operation.
  - How long do we keep data? App data is deleted promptly on uninstall ([app/uninstalled](#) / [shop/redact](#)); encrypted backups purge within 30 days. Brokerage records (including carrier POD/tracking) are kept  $\geq 5$  years as required for audits/compliance.
  - Children? The Services are not for individuals under 18.
  - Where is data stored? In the United States; our primary database server is in California.
  - Your rights. We honor privacy rights where required by law (e.g., GDPR/UK, California). Contact [hello@forgehq.com](mailto:hello@forgehq.com).
- 

## 1) What Information Do We Collect?

### A. Personal information you disclose to us

In short: Business contact information you provide.

We collect information you voluntarily provide—e.g., merchant name, work email, phone, company, job title, and your messages to support or sales. If you receive our marketing emails, you can unsubscribe at any time.

We do not operate a separate customer portal outside Shopify, and we do not store card/bank numbers. Our brokerage is compensated from drawback refunds (contingency basis).

### B. Information collected automatically

In short: Only what's necessary to operate securely.

We may collect essential technical information when you visit or use the Services (e.g., IP address at runtime, device/browser type, pages requested) to keep the Services secure and functioning. We do not set analytics or advertising pixels and we do not persist hosting/platform logs.

Cookies & similar technologies. We do not set non-essential cookies. The site may use strictly necessary cookies for secure sessions/load balancing.

## C. Information collected from other sources

In short: Shopify (app) and carriers (brokerage).

- From Shopify (when you install our app): We sync orders, fulfillments, products, and inventory fields needed to prepare drawback claims (e.g., order IDs, line items/SKUs/variants, quantities, prices/taxes/duties, timestamps, inventory adjustments). We do not retain consumer contact data (such as recipient name, address, email, or phone) from order payloads.  
Webhook audit trail (minimal): we record only the webhook topic (e.g., [orders/create](#)), shop domain, and time received; we do not store the webhook payload.
- From carriers (brokerage only, outside the app): With merchant authorization, we obtain proof-of-delivery (POD) and tracking information directly from carriers (e.g., FedEx, UPS, DHL). Carrier PODs may include tracking number, delivery status/timestamp, destination details, and, depending on the carrier, recipient name/address/signature.

## D. Sensitive information

We do not collect biometric, health, or similar sensitive categories. Brokerage files may include government/business identifiers necessary for customs compliance. We do not collect passport/ID scans or SSNs.

---

# 2) How Do We Process Your Information?

In short: To provide, secure, and improve the Services; to comply with law.

We process information to:

- Deliver the Services and prepare/organize records for U.S. duty drawback
- Provide support and respond to inquiries
- Send administrative messages (service, legal, or security notices) and business/feature updates to merchant contacts (you may opt out via the unsubscribe link)
- Protect, investigate, and prevent security incidents or abuse

- Comply with legal/regulatory obligations (e.g., customs/drawback recordkeeping and audits)
- For other purposes with your instruction or as required by law

We do not use data for targeted behavioral advertising.

---

### 3) What Legal Bases Do We Rely On (EU/UK)?

Where GDPR/UK GDPR applies, we process your information under:

- Contract (to provide the Services you request)
- Legitimate interests (security, service reliability, audit defense), balanced against your rights
- Legal obligation (customs/drawback recordkeeping and responding to lawful requests)

International transfers. We host data in the U.S.. For EEA/UK transfers, we use the EU Standard Contractual Clauses (and UK addendum) as appropriate.

---

Controller basis for legally required retained copies. For the retained copies we must keep for brokerage/legal compliance (e.g., POD/tracking/filings), Forge acts as an independent controller and relies on legal obligation and/or legitimate interests (audit defense and compliance).

#### 4. When and With Whom Do We Share Personal Information?

In short: With service providers and when legally required—never for ads.

- Service providers (processors/subprocessors). Categories include cloud hosting/storage, databases/backups, monitoring, email/helpdesk, and similar operations. They may only use information to perform services for us and are bound by

confidentiality and data-protection terms.

- Authorities & legal. When required by law, regulation, or legal process, or to protect rights and safety.
- Business transfers. If we undergo a merger, acquisition, or asset sale, information may be transferred under this notice.

We do not sell personal information and do not share it for cross-context behavioral advertising.

---

## 5) Do We Use Cookies or Other Tracking Technologies?

In short: No non-essential cookies or pixels. We may use strictly necessary cookies to operate the site securely (e.g., session or load-balancer cookies). We do not deploy analytics or advertising cookies/pixels.

---

## 6) How Do We Handle Social Logins?

Not applicable. We do not offer social logins.

---

## 7) How Long Do We Keep Your Information?

In short: Only as long as needed, then delete or anonymize.

- Shopify app data. Retained while the app is installed and merchant's account is active. Upon receiving **app/uninstalled** and/or **shop/redact**, we promptly delete active copies. Encrypted backups purge within 30 days.
- Webhook audit trail. Entries are treated as app data and follow the uninstall deletion and 30-day backup purge policy.
- Brokerage/drawback records (including carrier POD/tracking). Retained at least five (5) years from creation (or longer if required by law/contract) for audits and legal compliance, then deleted or anonymized. We act as an independent controller for these

retained copies under legal obligation/legitimate interests.

- Marketing contacts (merchant business emails). Kept while your business relationship is active and for up to 24 months after the last interaction, unless you unsubscribe sooner.

We do not persist hosting/platform logs.

---

Legal acceptance records. We maintain a minimal record of legal acceptance (shop domain, timestamp, and document versions accepted) for audit purposes. These records are deleted on uninstall and included in the 30-day encrypted-backup purge schedule.

#### 8. How Do We Keep Your Information Safe?

In short: Organizational and technical safeguards.

We use appropriate measures, including encryption in transit and at rest, least-privilege access controls, monitoring, and backups. No system is 100% secure; transmission is at your own risk. Access to carrier documents and records is restricted.

---

## 9) Do We Collect Information From Minors?

In short: No. The Services are not directed to individuals under 18.

By using the Services, you represent you are at least 18. If we learn we collected information from someone under 18, we will deactivate any related account (if applicable) and promptly delete the data. Contact [hello@forgehq.com](mailto:hello@forgehq.com).

---

## 10) What Are Your Privacy Rights?

Your rights depend on your location and applicable law. Where required (e.g., GDPR/UK GDPR, California), you may have rights to access, correct, delete, receive a copy (portability), appeal a

decision, and opt-out of sales/sharing (we do not sell/share). To exercise rights, email [hello@forgehq.com](mailto:hello@forgehq.com).

Verification. We verify requests via a logged-in merchant admin (if applicable) or by matching your business email/domain, and may request limited additional information to confirm identity/authority.

Authorized agents & appeals. We accept requests from authorized agents with written permission. If we decline a request, you may appeal via [hello@forgehq.com](mailto:hello@forgehq.com).

Consumers of merchants. If you are a consumer of a merchant that uses our app, please contact the merchant directly. We support merchants by honoring Shopify privacy webhooks ([customers/data\\_request](#), [customers/redact](#), [shop/redact](#)).

---

## 11) Controls for Do-Not-Track (DNT) & Global Privacy Control (GPC)

We do not engage in cross-site tracking or behavioral advertising and do not set non-essential cookies. DNT signals therefore do not change how we process data. Where applicable law recognizes GPC signals, we honor them. We do not sell or share personal information for cross-context behavioral advertising.

---

## 12) Do United States Residents Have Specific Privacy Rights?

In short: California and certain other states grant additional rights.

### Notice at Collection (California) – Summary

We collect the following categories of personal information for the purposes and retention periods shown. We do not sell or share personal information for cross-context behavioral advertising.

Category (CPRA)	Examples	Collected	Retention
-----------------	----------	-----------	-----------

A. Identifiers	Merchant business contact (name, work email/phone), shop domain, tracking numbers	Yes	Business contact: account duration + 24 months; App data: delete on uninstall (backups ≤ 30 days); Brokerage POD/track: ≥ 5 years
B. Customer Records (contact)	Merchant business contact details	Yes	Account duration + 24 months
D. Commercial information	Order/line-item details, duty/tax amounts, inventory adjustments; carrier POD/tracking (brokerage)	Yes	App data: delete on uninstall (backups ≤ 30 days); Brokerage: ≥ 5 years
I. Professional or employment info	Company, job title (B2B context)	Yes	Account duration + 24 months
All other categories (C, E, F, G, H, J, K, L Sensitive)	—	No	—

Sources. Directly from you; from Shopify (merchant-authorized scopes) for app data; and directly from carriers for brokerage POD/tracking.

Purposes. Provide and secure the Services; prepare drawback claims; comply with law; maintain records; communicate with you.

Sale/Share. No.

---

## 13) Changes to This Notice



We may update this notice from time to time. The updated version will be indicated by an updated “Last updated” date. If we make material changes, we may notify account contacts by email or in-product notice.

---

## 14) How to Contact Us

Forge Technologies Inc.  
2261 Market St STE 86068  
San Francisco, CA 94114  
Email: [hello@forgehq.com](mailto:hello@forgehq.com)

---

## 15) How to Review, Update, or Delete the Data We Collect

Submit a request to [hello@forgehq.com](mailto:hello@forgehq.com). If you are a consumer of a merchant that uses our app, please contact the merchant directly; we will assist them by honoring Shopify privacy webhooks.

---

## App-Specific Notes (Shopify)

- Scopes requested: [read\\_inventory](#), [read\\_locations](#), [read\\_orders](#), [read\\_products](#), [read\\_all\\_orders](#)
  - Webhooks consumed: [orders/create](#), [orders/updated](#), [fulfillments/create](#), [fulfillments/updated](#), [inventory\\_levels/update](#), and Shopify privacy webhooks ([customers/data\\_request](#), [customers/redact](#), [shop/redact](#))
  - Data minimization: We retain no consumer contact data from orders; only fields needed for drawback prep
  - Uninstall deletion & backups: Active app data is deleted promptly on uninstall or [shop/redact](#); backups purge within 30 days
  - Webhook audit trail: topic + shop domain + time received; no payload stored
-

## Brokerage / Duty Drawback (Outside the App)

For brokerage clients, we process commercial and customs data—including carrier POD and tracking obtained directly from carriers with your authorization—solely to substantiate exports/deliveries and comply with law. These records are retained ≥ 5 years (or longer if required). We may disclose to authorities when legally required. For these retained copies, Forge acts as an independent controller under applicable data protection laws.

---

## 16) Data Processing Addendum (Processor Terms for Merchant Customers)

This section forms part of this Privacy Policy and your Agreement with Forge.

Additional processor terms (clarifications):

- Documented instructions. Merchant instructs Forge to process (i) Shopify orders, fulfillments, products, and inventory fields necessary to prepare U.S. duty-drawback claims; (ii) a minimal webhook audit trail consisting of topic, shop domain, and time received (no payload retained); and (iii) for brokerage clients only, carrier proof-of-delivery (POD) and tracking obtained directly from carriers under Merchant authorization.
- Role split. Except as stated, Forge acts as a processor/service provider to Merchant. For records Forge is legally required to retain (e.g., carrier POD/tracking and drawback filings), the parties acknowledge Forge acts as an independent controller for those retained copies and uses them solely for legal/compliance purposes.
- EU/UK transfers. The EU Standard Contractual Clauses (Controller-to-Processor, Module 2) – Commission Decision (EU) 2021/914 and the UK Addendum/IDTA are incorporated by reference between Merchant (exporter) and Forge (importer). Annex details are as set out in this Policy/DPA; the competent supervisory authority is that of Merchant's EEA establishment (or Ireland if uncertain).
- CPRA service-provider certification. Forge certifies it understands and will comply with CPRA service-provider requirements, including processing only for the limited business purposes described, no selling or sharing, deleting/returning data on request, assisting with consumer requests, and imposing equivalent obligations on subprocessors.\*  
Parties. This Data Processing Addendum ("DPA") forms part of the Agreement between Forge Technologies Inc. ("Forge") and the merchant ("Merchant").

**Roles.** Merchant is the controller/business; Forge acts as processor/service provider for personal data that Merchant provides or authorizes Forge to obtain to deliver the Services (including any Forge Shopify app and duty-drawback/brokerage work).

**Scope & Instructions.** Forge will process personal data only on Merchant's documented instructions: to provide, secure, and support the Services; to organize records for U.S. duty drawback; to comply with law; and as otherwise permitted by this DPA.

**Data Minimization.** For the Shopify app, Forge retains no consumer contact data from orders and stores only fields needed for drawback preparation (e.g., order/line items/SKU, quantities, duty/tax amounts, timestamps, inventory adjustments). Forge keeps a minimal webhook audit trail of topic, shop domain, and time received; no payload is stored. Carrier POD/tracking used for brokerage is obtained directly from carriers (e.g., FedEx, UPS, DHL) under Merchant authorization.

**Confidentiality & Security.** Forge ensures personnel are bound by confidentiality and implements appropriate technical and organizational measures, including encryption in transit and at rest, least-privilege access controls, monitoring, and backups.

**Subprocessors.** Forge may use subprocessors to provide the Services and will ensure they are bound by written terms no less protective than this DPA. Forge remains responsible for their performance.

**Assistance & Requests.** Forge will reasonably assist Merchant with data-subject requests and legal obligations applicable to Merchant. Forge honors Shopify privacy webhooks: [customers/data\\_request](#), [customers/redact](#), and [shop/redact](#).

**Deletion & Return.** Upon uninstall or [shop/redact](#), Forge will promptly delete Merchant's app data from active systems or return it upon request; encrypted backups purge within 30 days of deletion. Brokerage/drawback records may be retained ≥ 5 years where required by law or contract and will be protected under this DPA.

**International Transfers.** Forge hosts data in the United States (primary database in California). Where the GDPR/UK GDPR applies to transfers from the EEA/UK, the parties rely on the EU Standard Contractual Clauses and the UK Addendum.

**Breach Notification.** Forge will notify Merchant without undue delay after becoming aware of a personal-data breach affecting Merchant data and will cooperate to mitigate and remediate.

**Audits & Information.** On reasonable request, Forge will provide information necessary to demonstrate compliance with this DPA. Formal audits occur only where required by law/regulator and are subject to confidentiality and safety measures.

Service-Provider/No Sale. Forge will not sell personal information and will not share it for cross-context behavioral advertising. Processing is limited to providing the Services.

Order of Precedence. If this DPA conflicts with the Agreement on privacy/security matters, this DPA controls; otherwise the Agreement's governing law, venue, and liability terms apply.