

Data Classification and Encryption Policy

Last updated October 23, 2026

This policy explains how Bump The DSL, LLC, the company that builds and operates Relay (“we”) classifies information by sensitivity, and the protections, including encryption, that each class requires. It applies to all information we create, receive or store, including data received from Shopify and TikTok Shop.

SUMMARY

Credentials and personal data are our most sensitive data. They are always encrypted in transit and at rest, and the most sensitive personal fields get an extra layer of encryption on top of the database's own.

Classification levels

Level	Examples	Required handling
Restricted	Passwords, API keys and secrets, platform access tokens (for example Shopify and TikTok Shop), encryption keys	Kept only in a secret manager or password manager; encrypted; never logged, emailed or shared; rotated whenever exposure is suspected
Confidential	Personal data: customer order and contact details, creator names, emails, phone numbers, shipping addresses, messages and notes, and any data received from TikTok Shop; financial records	Encrypted in transit and at rest; direct identifiers additionally encrypted at field level; least-privilege access; retention limits

Level	Examples	Required handling
Internal	Non-personal business data: sales totals, ad performance, product and inventory data, internal documents	Staff only; not published
Public	Website content, published policies	No restrictions

Encryption in transit

All traffic to and from our systems uses TLS (HTTPS), and plain HTTP is redirected. Connections to our database require TLS, and our calls to platform APIs such as Shopify and TikTok Shop are made over HTTPS.

Encryption at rest

- **Database storage** is encrypted at rest by our database provider.
- **Field-level encryption.** Platform access tokens and the most sensitive personal data (creator contact details, shipping addresses, messages and notes, and dispute evidence that names a person) are also encrypted by Relay with AES-256-GCM before they are saved. The keys are separate for each kind of data and are held apart from the database.
- **One-way hashing.** API tokens, and the values we only need to match against, are stored as one-way or keyed hashes, so the original value is never kept.
- **Company computers** use full-disk encryption.

Key management

- Keys are generated randomly with at least 256 bits of strength.
- Keys are stored only in our hosting provider's secret manager, with a backup in the owner's password manager. They are never in code or documents.
- Keys are rotated whenever exposure is suspected. Relay supports moving to a new key without losing access to existing data.

Handling rules

- Restricted and Confidential data stays in approved systems. It is not copied into email, chat, spreadsheets or AI tools unless that is approved and necessary.

- Exports contain only the fields needed, and are deleted once they have been used.
- Development and testing use made-up data, never production personal data.

Retention and disposal

We keep Confidential data only as long as it is needed, and much of it is deleted automatically on a schedule. For example, a creator's shipping address is erased a set number of days after their sample is delivered, message and note text is deleted after a set retention period, and platform notification records are deleted after 30 days. Devices are securely wiped before they are reused or disposed of. Our Personal Data Protection Policy explains retention in more detail.

Review of this policy

This policy is reviewed at least once a year and whenever we add a system, change how we use personal data, or learn something from an incident. The next scheduled review is October 2027. Version 1.0, first published October 23, 2026.

Contact

Questions about this policy can be sent to privacy@bumptheds1.com.