ENTERPRISE SECURITY · BUILT FOR REGULATED CONTENT

# Security by design. Protection at every layer.

Enterprise-grade security controls protect your data across every layer of its flow. Regular internal and external penetration testing assesses our backend infrastructure. Every client's data is logically segregated, access is scoped to their organization, and all LLM requests are routed exclusively over secured connections.

**0%**

## of your content is ever used to train or fine-tune a model.

Prompts and metadata are processed transiently to return your translation and are not retained by our model vendors. You set the data-retention policy for your organization, down to zero.

AI & CLIENT DATA · A ZERO-TRAINING COMMITMENT

HOW WE PROTECT YOUR DATA

## Defense in depth, across every layer.

Controls span the network, identity, data and monitoring layers, so a single failure is never a single point of exposure.

01 NETWORK & INFRASTRUCTURE

### Security by Design

Protection is engineered into every layer of the data flow, not bolted on afterward.

- ✓ Internal and external penetration testing
- ✓ Client data segregated and access-scoped
- ✓ LLM requests over secured connections only
- ✓ Network segregation and access restriction

02 AI & CLIENT DATA

### Your Data Stays Yours

Your content is used to serve you, and for nothing else.

- ✓ Never used to train or fine-tune any model
- ✓ Processed transiently for your translation
- ✓ Prompts and metadata never retained
- ✓ You control data retention, down to zero

03 ACCESS CONTROL

### Authentication & Authorization

Access is granted narrowly, verified strongly, and never shared.

- ✓ Least-privilege role-based access control
- ✓ Multi-factor authentication enforced
- ✓ API keys and tokens stored securely

04 AUDIT & MONITORING

### Logged & Reviewable

Every action leaves a record that can be independently reviewed, at any time.

- ✓ Every access event and API call is logged
- ✓ Full logs are reviewable on demand
- ✓ Regular privileged-access reviews

ENCRYPTION EVERYWHERE

**TLS 1.2 / 1.3**

DATA IN TRANSIT

Encryption, authentication and message integrity on every connection.

**AES-256**

DATA AT REST

Contents, databases and backups are all encrypted.

CERTIFICATIONS & ATTESTATIONS

## Independently assessed. Continuously aligned.

| | |
|---|---|
| **SOC 2 Type I** ACHIEVED | Independent auditor's report on the design and implementation of security controls, covering Security, with Confidentiality and Availability in scope. |
| **SOC 2 Type II** PLANNED Q4 2026 | In planning and preparation for Q4 2026. The report tests that controls operate effectively over time. |
| **ISO / IEC 27001** ALIGNED | Our information security management system is designed in alignment with ISO/IEC 27001, organizing cybersecurity around Organization, People, Process and Technology. |
| **NIST CSF 2.0** ALIGNED | The NIST Cybersecurity Framework 2.0 is our reference model for control set and maturity tracking, mapped to its core functions per security best practices. |
| **GDPR · Law 25 · PIPEDA** ALIGNED | Fully aligned with the EU GDPR, Quebec's Law 25 and Canada's PIPEDA to ensure data security, protection and privacy. |

Certifications and attestations are maintained by TRSB, the parent organization behind OTTO, covering the infrastructure and controls on which OTTO operates.