Fox ML Infrastructure – Data Processing Addendum (DPA)

This Data Processing Addendum ("DPA") clarifies how Fox ML Infrastructure handles (or, more accurately, does not handle) client data.
This document is designed for enterprise legal teams and procurement departments evaluating data privacy and compliance.

---

1. Executive Summary

Fox ML Infrastructure does not process, store, retain, or transmit client data.

The platform is **client-hosted software** that runs entirely within the client's infrastructure. Fox ML Infrastructure LLC has no access to client data, no ability to process client data, and no infrastructure that could store or transmit client data.

We will never sell client data. This is a permanent commitment to protecting client privacy. Even in the event that any data is collected (limited to licensing and support communications), it will never be sold, rented, traded, or monetized in any way.

---

2. Data Processing Status

2.1 No Data Processing

Fox ML Infrastructure does not process client data.

- **No data storage** – Fox ML Infrastructure does not store any client data
- **No data retention** – Fox ML Infrastructure does not retain any client data
- **No data transmission** – Fox ML Infrastructure does not transmit any client data to third parties or external systems
- **No data access** – Fox ML Infrastructure does not have access to client production data

2.2 Client-Hosted Architecture

All data processing occurs on client-owned hardware.

- Software runs entirely within the client's infrastructure
- All data remains on client-controlled systems
- Client manages all data storage, networking, and access control
- No vendor access to client systems or data

---

3. Data Handling Practices

3.1 No Telemetry or Analytics

Fox ML Infrastructure does not collect usage data or telemetry.

- **No telemetry** – The platform does not send usage data, analytics, or tracking information to external services
- **No analytics** – No user behavior tracking, no performance metrics collection, no feature usage tracking
- **No outbound calls** – The platform does not make outbound network calls (except as configured by the client for data sources)
- **No embedded trackers** – No third-party tracking scripts, pixels, or analytics tools

3.2 No Data Collection

Fox ML Infrastructure does not collect any data.

- **No user data** – No user accounts, no login information, no user preferences
- **No operational data** – No logs transmitted externally, no error reports sent to vendor
- **No model data** – No model outputs, predictions, or results transmitted externally
- **No trading data** – No trading signals, positions, or financial data collected

---

4. Consulting Engagements

4.1 Limited Data Access

For consulting engagements only (separate from licensing):

- **NDA required** – All consulting engagements require a Non-Disclosure Agreement
- **Limited scope** – Data access is limited to the minimum required for the engagement
- **Client-controlled** – All data access uses client-approved secure methods
- **No retention** – Client data is deleted upon project completion unless written authorization is provided

See `LEGAL/consulting/SECURITY_AND_ACCESS_POLICY.md` **for detailed consulting security practices.**

4.2 Data Handling for Consulting

When consulting engagements require data access:

- Data is accessed only for the duration of the project
- Data is stored only in client-approved environments
- No data is transferred to personal cloud storage or external services
- All datasets, credentials, and artifacts are deleted upon delivery

---

5. Code Delivery

5.1 Private Repository Access

Commercial licenses include access to private GitHub repositories.

- Code is delivered via private, client-specific repositories
- Access is controlled via GitHub organization or repository-level permissions
- No client data is included in code repositories
- Client-specific configurations remain in client-controlled repositories

5.2 No Production Access

Fox ML Infrastructure does not access client production systems.

- No vendor access to production environments
- No vendor access to production API keys or credentials
- No vendor access to trading accounts or financial systems
- All deployment and operations are client-controlled

---

6. Compliance Principles

6.1 GDPR Principles

Fox ML Infrastructure adheres to GDPR principles (even if not legally required as a data processor):

- **Data minimization** – No data is collected, so no unnecessary data processing
- **Purpose limitation** – No data processing occurs, so no purpose limitation concerns
- **Storage limitation** – No data is stored, so no retention concerns
- **Integrity and confidentiality** – Client data remains fully client-controlled
- **Accountability** – Clear documentation of data handling practices

6.2 CCPA Principles

Fox ML Infrastructure adheres to CCPA principles:

- **No data collection** – No personal information is collected
- **No data sale** – No data is sold, rented, traded, or monetized – now or ever
- **Permanent commitment** – We will never sell client data, regardless of business model changes
- **Client control** – All data remains under client control
- **Transparency** – Clear documentation of data handling practices

This is a permanent, non-negotiable commitment to client privacy protection.

---

7. Third-Party Services

7.1 No Third-Party Data Transmission

Fox ML Infrastructure does not integrate with third-party vendor services.

- No external API calls (except as configured by the client for data sources)
- No vendor-hosted services
- No third-party analytics or telemetry
- No data transmission to external systems

7.2 Client-Configured Data Sources

Clients may configure data sources (e.g., market data APIs):

- These connections are client-configured and client-controlled
- Data flows directly from source to client systems
- Fox ML Infrastructure does not intercept, store, or process this data
- Client is responsible for compliance with data source terms

---

8. Security and Access Control

8.1 No Vendor Access

Fox ML Infrastructure does not have access to client systems or data.

- No vendor access to production environments
- No vendor access to client credentials or API keys
- No vendor access to trading accounts or financial systems
- All access control is client-managed

8.2 Client-Controlled Security

Clients control all security measures:

- Client manages all authentication and authorization
- Client controls all network security and firewalls
- Client manages all encryption and key management
- Client is responsible for all security compliance

---

9. Data Subject Rights

9.1 No Data Processing Means No Data Subject Rights Requests

Since Fox ML Infrastructure does not process client data:

- No data subject access requests are necessary
- No right to deletion requests (no data to delete)
- No right to rectification requests (no data to correct)
- No data portability requests (no data to export)

All data subject rights are managed by the client, as the client is the data controller.

---

10. Data Breach Notification

10.1 No Vendor Data Breach Risk

Since Fox ML Infrastructure does not store or process client data:

- No vendor data breach can expose client data
- No vendor security incident can compromise client data
- Client data remains secure within client-controlled infrastructure

10.2 Client Data Breach Responsibility

Clients are responsible for:

- Securing their own infrastructure
- Managing their own data access controls
- Complying with data breach notification requirements
- Maintaining their own security practices

---

11. Subprocessors

11.1 No Subprocessors

Fox ML Infrastructure does not use subprocessors for data processing.

- No third-party data processors
- No cloud service providers for data storage
- No analytics providers
- No data transmission services

Since no data processing occurs, no subprocessors are involved.

---

12. International Data Transfers

12.1 No International Data Transfers

Fox ML Infrastructure does not transfer data internationally.

- No data is transferred across borders
- No data is stored in international locations
- All data remains in client-controlled infrastructure
- Client determines all data location and transfer decisions

---

13. Summary

Key Points:

1. **No data processing** – Fox ML Infrastructure does not process, store, retain, or transmit client data
2. **Client-hosted** – All software runs on client-owned hardware
3. **No telemetry** – No usage data, analytics, or tracking
4. **No vendor access** – No access to client production systems or data
5. **Client-controlled** – All data remains under client control
6. **Compliance-ready** – Adheres to GDPR/CCPA principles even if not legally required

This architecture ensures that Fox ML Infrastructure operates as a zero-data-processing platform, eliminating privacy concerns and compliance complexity.

Contact

For questions about data processing or privacy:

Jennifer Lewis
Fox ML Infrastructure LLC
Email: **jenn.lewis5789@gmail.com**
Subject: *Data Processing Addendum Inquiry – Fox ML Infrastructure*

Related Documents

- `LEGAL/SECURITY.md` – Security statement and data handling practices
- `LEGAL/consulting/SECURITY_AND_ACCESS_POLICY.md` – Detailed security practices for consulting engagements
- `LEGAL/ENTERPRISE_DELIVERY.md` – Repository structure and delivery model
- `COMMERCIAL_LICENSE.md` – Commercial license terms