## General Statement

All data that are generated and stored on the MQO A.I. Hub (except for content that actively shared by using a "public share" feature) are encrypted (AES-256, "CBC mode") such that even we (MQO Research) cannot view the contents of your data (including Prompts, GPT Responses, Chat Histories, uploaded audio or video files, transcriptions, or any other content). Per our Data Processing Agreement (DPA) and MQO's Healthcare Addendum stipulating "Zero Data Retention" in line with PIPEDA/HIPAA compliance, your data will not be shared, monetized, or used for training of A.I. models. All data generated and stored on the MQO A.I. Hub are subject to our Terms of Use, Privacy Policy, and above-mentioned DPA and Addendum with OpenAI. The OpenAI API has been evaluated by a third-party security auditor and is SOC 2 Type 2 compliant. All user-produced data are stored in encrypted format on our servers located in Canada.

## Common Questions

### 1. What is the dependency on external APIs or cloud services?

- Canadian-hosted compute servers with AWS and Microsoft Azure (encrypted in transit; no data stored at rest)
- Canadian-hosted data servers with AWS and Wasabi (encrypted at rest and in transit, see below)
- OpenAI API (US-based, but PIPEDA/HIPAA-compliant zero data retention workflow; encrypted in transit; no data stored at rest)

### 2. What encryption standards are used? Are data encrypted in transit or only at rest?

AES-256 "CBC mode" (cipher block chaining), at rest; TLS 1.2+ / "GCM mode" (Galois/Counter) in transit.

### 3. Does the platform send usage data, crash reports, or any other telemetry to external servers?

Yes, aggregated usage data, access logs, and crash event logs are stored on our platform's Canadian-based servers. These are stored in encrypted format and no original content/data could be reverse engineered or inferred from the collected data.

### 4. Are any data automatically stored or recorded? Does the platform automatically delete temporary files or data caches?

When an Organization account is created on the platform, this produces an environment that is encrypted at the Organization level. The Organization's Owner account login information is the decryption key for the Organization's environment. All Users created through the Organization operate within the Organization's encryption (therefore MQO, nor our upstream partners, can access unencrypted data produced on the platform).

To enable users to access their own data generated on the platform, these data are stored by the platform in encrypted format. Any data deleted by a user on the platform are fully and irreversibly deleted on the server. The "Content Centre" module on the platform enables users to view a stream of all data they produce on the platform across all modules, with option to delete any content. Any real-time processing that makes use of cache data that are not stored, are never written to persistent storage and are immediately cleared from server RAM upon completion or termination of the process.

*This document contains a single page.*