DIAPTORAI SYSTEM - BETA TERMS AND DATA HANDLING NOTICE

Draft for legal review – not final legal text

Last updated: Tuesday, 2 June 2026

1. Beta Nature of the Service

This service is currently provided as a limited beta system based on the TIRE Protocol: Truth, Integrity, Responsibility, Ethics.

The service is not itself a standalone artificial intelligence model. It operates as an interface, reasoning framework, and processing layer that uses external artificial intelligence providers through API-based services where needed. As a result, user inputs, chat content, uploaded document extracts, and related processing data may be transmitted to external AI providers or infrastructure providers when necessary to provide the service.

The service is designed to support critical reasoning, structured evaluation, document-assisted analysis, and interaction with AI systems under explicit epistemic limits.

The service may include different functional areas, including but not limited to Answer, Verify, and future reasoning or brainstorming tools. Some features may use chat-style continuity, while others may process individual verification requests, structured evaluations, uploaded content, or source-assisted checks. Data handling may differ depending on the functional area and the feature used.

The service is not a substitute for professional legal, medical, financial, psychological, technical, or other expert advice. Users remain responsible for how they interpret and use the outputs.

Because the system is in beta, features, data handling practices, retention periods, interface elements, technical safeguards, and terms of use may change as the platform is tested, improved, and reviewed.

Where changes materially affect user rights, data handling, retention, security, or user obligations, users will be informed and may be required to review and accept the updated terms before continuing to use the service.

Chat data and uploaded document content-processing files are encrypted at rest. Operational metadata may remain readable where necessary for the service to function. This encryption framework remains under technical review and may be further strengthened before wider beta access where required.

2. AI Limitations and User Responsibility

The system may generate incomplete, uncertain, or incorrect outputs.

The TIRE Protocol is designed to reduce unjustified certainty, hallucination, and misleading plausibility, but it cannot eliminate the possibility of error.

Users must not rely on the service as the sole basis for decisions that may affect rights, safety, health, finances, legal obligations, employment, reputation, human relationships, or other significant interests.
Where appropriate, users should verify outputs independently and seek qualified professional advice.

3. User Accounts and Access

Access to the beta may be limited, manual, or invitation-based.

Users are responsible for maintaining the confidentiality of their credentials and for notifying the service operator if they suspect unauthorized access.

The service operator may limit, suspend, or revoke access in case of misuse, security concerns, technical risk, or violation of these terms.

4. Storage, Export and Backups

Different areas of the service may use different storage and export models, depending on their function.

In areas that provide chat-style continuity, such as Answer, chats may be stored so that users can continue previous conversations and so that the system can maintain structured continuity.

Stored chat-related data may include, depending on the feature used:

- chat history;
- structured memory or summaries;
- technical identifiers;
- timestamps;
- conversation metadata;
- system-generated continuity, retrieval, or source-tracking aids;
- references to uploaded documents;
- citations, source references, or excerpts discussed within a chat.

Some files may currently use protected or internal storage formats.

The service may provide official export functions. In chat-style areas, the official verified export beta may include:

- chat text;
- integrity metadata, including a canonical hash;
- a deduplicated source summary with used_in_turns;
- references to user-uploaded documents when such documents were considered as sources or semantic context.

The official verified export beta for chat-style areas does not include the uploaded documents themselves, full extracted document text, internal semantic document summaries, or full internal retrieval/evidence structures, unless expressly stated in a specific export version.

In non-chat evaluation areas, such as Verify, evaluations may be atomic rather than conversational. A Verify evaluation may include user-provided text, uploaded document text extracted for that evaluation, textual visual interpretation generated from an uploaded image, retrieved sources, evaluation labels, model output, technical metadata, timestamps, and integrity data.

The service may provide an Official Verify Copy for a single Verify evaluation. An Official Verify Copy is generated by the service for that evaluation and may include the full material needed by the user to preserve the evaluation record, including:

- the question or context;
- the text submitted for verification;
- uploaded document filename and extracted text, where used in the evaluation;
- uploaded image filename and the textual visual interpretation generated from it, where used in the evaluation;
- retrieved source references or source summaries;
- the Verify output;
- technical metadata;
- integrity metadata, including canonical hashes.

For Official Verify Copies, the complete readable copy is intended to be held by the user. The service may retain only a minimal technical audit record, such as identifiers, timestamps, user

identifier, canonical hashes, retrieval status, source counts, and related integrity metadata. Unless expressly stated otherwise, the service does not retain the readable contents of the Verify evaluation in this audit record.

HMAC-based verification or digital signatures may be added in future export versions.

Copies made manually by users, including screenshots, pasted excerpts, browser copies, copied messages, or edited files, may not be technically verifiable by the service as complete, authentic, or unmodified. Where an official export or Official Verify Copy is available, that official copy is the reference format intended for later technical integrity checks.

Chat data encryption at rest has been implemented and remains under technical review. It may be further strengthened before wider beta access where required.

For continuity and disaster recovery, encrypted backups of chat and memory data may be retained for a limited backup-retention period. Such backups are not intended for ordinary user access, profiling, or model training.

Uploaded original documents and related document content-processing files are not intended to be included in ordinary chat backup processes.

In Verify or other non-chat evaluation areas, the service may process verification inputs, outputs, evaluation labels, technical metadata, timestamps, logs, source references, and related records where needed to provide the feature, maintain security, support debugging, or preserve service integrity.

5. Deleting Chats

Deleting a chat may immediately remove it from the user interface and starts the applicable deletion process for that chat.

Before a stored chat can be deleted, the service requires generation of an official verified export of that chat. This requirement is intended to preserve a system-generated record before deletion and to reduce disputes based on manual, incomplete, edited, or unverifiable copies. The user remains responsible for downloading and keeping any export they wish to retain. Manual copies, screenshots, copied messages, browser copies, or edited files are not official verified exports and cannot be technically verified by the service as complete, authentic, or unmodified.

Official verified exports may include system-generated integrity metadata, such as cryptographic hashes, signatures, timestamps, identifiers, or similar technical verification data.

Manual copies, screenshots, pasted excerpts, browser copies, or edited files may be useful for personal reference, but the service cannot technically verify them as complete, authentic, or unmodified.

Deleting a chat also deletes the documents associated with that chat: the original uploaded documents and their associated technical files are deleted according to the applicable deletion and retention policy.

Even after a chat is deleted from the active user interface, encrypted or otherwise protected copies may remain temporarily stored for a limited technical retention period, including within encrypted backup systems, for security, continuity, recovery, audit, abuse prevention, or dispute protection, until the applicable retention period expires.

After the applicable retention period, the system is intended to remove the stored readable chat content from the active system and retain only a minimal technical deletion record.

Such a minimal record may include:

- user ID;

- container ID;
- chat number or internal chat reference;
- timestamps;
- deletion event ID;
- deletion status;
- whether an official verified export was offered or generated;
- technical audit metadata;
- cryptographic hash, and, where implemented, signature, HMAC, or similar non-content verification record..

The purpose of such a record is to protect the integrity of the service and help address abuse, manipulation, fraud, disputes, recovery needs, or security incidents, without preserving the full readable chat content indefinitely in the active system.

6. Uploaded Documents

Users may upload documents for analysis within a chat.

Uploaded documents are used to support the conversation in which they are provided. The service must not be treated as a permanent archive, storage system, or backup service for users' original documents.

Uploaded original documents and related technical document files are not intended to be included in ordinary chat backup processes. Users remain responsible for keeping their own copies of any uploaded documents.

Uploaded documents may generate technical processing files needed for the service to work, including extracted text, document summaries, semantic structures, retrieval support files, metadata, and other processing artifacts.

As a general technical policy, the substantive contents of uploaded documents and derived document-content files, such as the original uploaded file, extracted text, and semantic document summaries, are encrypted at rest.

Operational metadata may remain unencrypted. This metadata may include information such as document identifier, filename, file type, upload time, expiry time, page count, character count, processing status, retention period, technical paths, hashes, and similar operational fields. This metadata is used for indexing, retention, deduplication, user interface display, troubleshooting, and system integrity.

Unless removed earlier by the user, uploaded documents and related technical document files are retained for a limited period, currently intended as 15 days, and are subject to automatic cleanup after expiry.

Deleting a chat deletes the uploaded documents associated with that chat, according to the applicable technical retention and deletion policy. Removing a document or deleting a chat does not necessarily remove text that has already become part of the chat itself, such as user messages, assistant responses, quotations, citations, summaries, or discussion of that document.

The service may exclude uploaded original documents and related technical document files from ordinary system backups. Users should therefore not rely on the service as a backup location for uploaded documents.

Documents and document-derived data may be processed by external artificial intelligence providers or infrastructure providers where this is necessary to provide the service. Users should not upload documents that they are not prepared to process through a beta system and through the technical providers required for that processing.

7. Removing Documents

The service may provide, or later introduce, functions allowing users to see which documents are associated with a chat and to remove a document from that chat.

When a document is removed, the service should remove the original uploaded file and related technical document files, subject to technical retention, security logs, and backup limitations described in this notice.

Removing a document does not necessarily remove text that has already become part of the chat, such as user messages, assistant responses, citations, summaries, or discussion of that document.

Deleting a chat deletes the documents associated with that chat, according to the applicable deletion and retention policy.

8. Image Uploads

The service may allow users to upload images for immediate analysis, discussion, verification, or contextual assistance within a chat.

Image uploads are handled separately from text-document uploads.

Unless expressly stated otherwise, uploaded images are intended to be used only in a volatile way for the immediate chat interaction. They are not intended to be stored by the service as persistent user documents, do not create extracted-text files, do not appear in the active documents list, and are not intended to be included in the official chat export. Images are not intended to be included in service backups.

The chat may still contain textual traces of the image interaction, such as the user's message, the assistant's response, descriptions, observations, or conclusions derived from the image. These textual chat contents may be stored, exported, deleted, backed up, or otherwise handled according to the ordinary chat management rules.

Uploaded images may be processed through external AI or infrastructure providers used to provide the requested image-understanding functionality. Temporary technical handling may occur where required to transmit, analyze, secure, debug, or provide the requested service.

Users should not upload images containing highly sensitive, private, confidential, or third-party personal data unless they have the right to do so and accept that the image may be processed through the technical providers used by the service.

Images may include personal or sensitive information even when this is not obvious, such as faces, minors, private locations, identity documents, medical information, vehicle plates, interiors, artworks, or other identifying details.

9. Backups

The service creates backups for continuity, security, and disaster recovery.

Backups may include application code, database dumps, configuration files, system metadata, and stored chat data.

Uploaded original documents and related technical document files may be excluded from ordinary backups, according to the backup policy in force.

Deleted or removed data may remain in protected backups for a limited time until those backups expire, rotate, or are overwritten.

Backups are not intended as user-accessible storage and should not be treated as an archive service for users.

10. Data Transit, AI Providers, Browser, and Security Boundaries

The service may rely on third-party infrastructure, web browsers, network services, and external AI providers in order to process user requests.

Information entered by the user, uploaded documents, prompts, outputs, technical metadata, or other data may be transmitted through such systems as necessary for the service to operate.

The processing of data by third-party AI providers, browser vendors, hosting providers, network services, or other technical intermediaries may be subject to their own terms, privacy policies, data processing agreements, security measures, and legal obligations.

The service operator will seek to use providers and configurations appropriate to the beta stage and to the risks involved, and relevant providers should be identified where applicable in the privacy documentation.

Users should not upload documents or provide information that they are not authorized to process through the service and its technical providers.

Users should also consider the security of their own device, browser, network connection, and account credentials. The service operator cannot control all risks arising from the user's local device, browser extensions, compromised accounts, insecure networks, or user-side storage of exported chats or copied content.

11. Sensitive Information

Users should avoid uploading or entering highly sensitive personal information unless strictly necessary for the intended use and unless they understand the current beta limitations.

Sensitive information may include, for example, health data, legal case materials, financial information, identity documents, confidential professional documents, information about minors, or data concerning third parties.

If such information is processed, users are responsible for ensuring that they have the right to provide it and that doing so is appropriate.

12. Logs and Technical Metadata

The service may keep technical logs and metadata for debugging, security, abuse prevention, cost monitoring, performance analysis, and service improvement.

The service should avoid unnecessary logging of user content.

During beta development, logging practices may be reviewed and reduced where they create unnecessary privacy risk.

13. User Rights and Data Requests

Users may request information about their data, correction of inaccurate data, deletion of data, or other applicable rights under data protection law.

Some requests may be subject to legal limitations, technical constraints, backup retention, security obligations, or legitimate defensive records.

Requests will be handled according to the applicable legal framework and the technical state of the beta system.

14. No Permanent Availability Guarantee

The service is provided in beta and may be interrupted, changed, suspended, or discontinued.

The operator does not guarantee permanent storage, permanent availability of chats, permanent access to uploaded documents, or uninterrupted service.

Users should keep independent copies of any material they consider important.

15. Acceptable Use

Users must not use the service to:

- violate applicable law;
- infringe the rights of others;
- upload material they are not authorized to process;
- attempt unauthorized access;
- bypass security controls;
- abuse system resources;
- submit malicious files or code;
- use the system for harmful, deceptive, or unlawful purposes.

16. Changes to These Terms

These beta terms and data handling practices may be updated as the system evolves.

Continued use of the service after changes may require renewed acceptance, depending on the nature of the update.

17. Legal Review

This document is a working draft for beta governance and legal review. It is not intended as final legal advice or a complete privacy policy until reviewed and approved by qualified legal counsel.