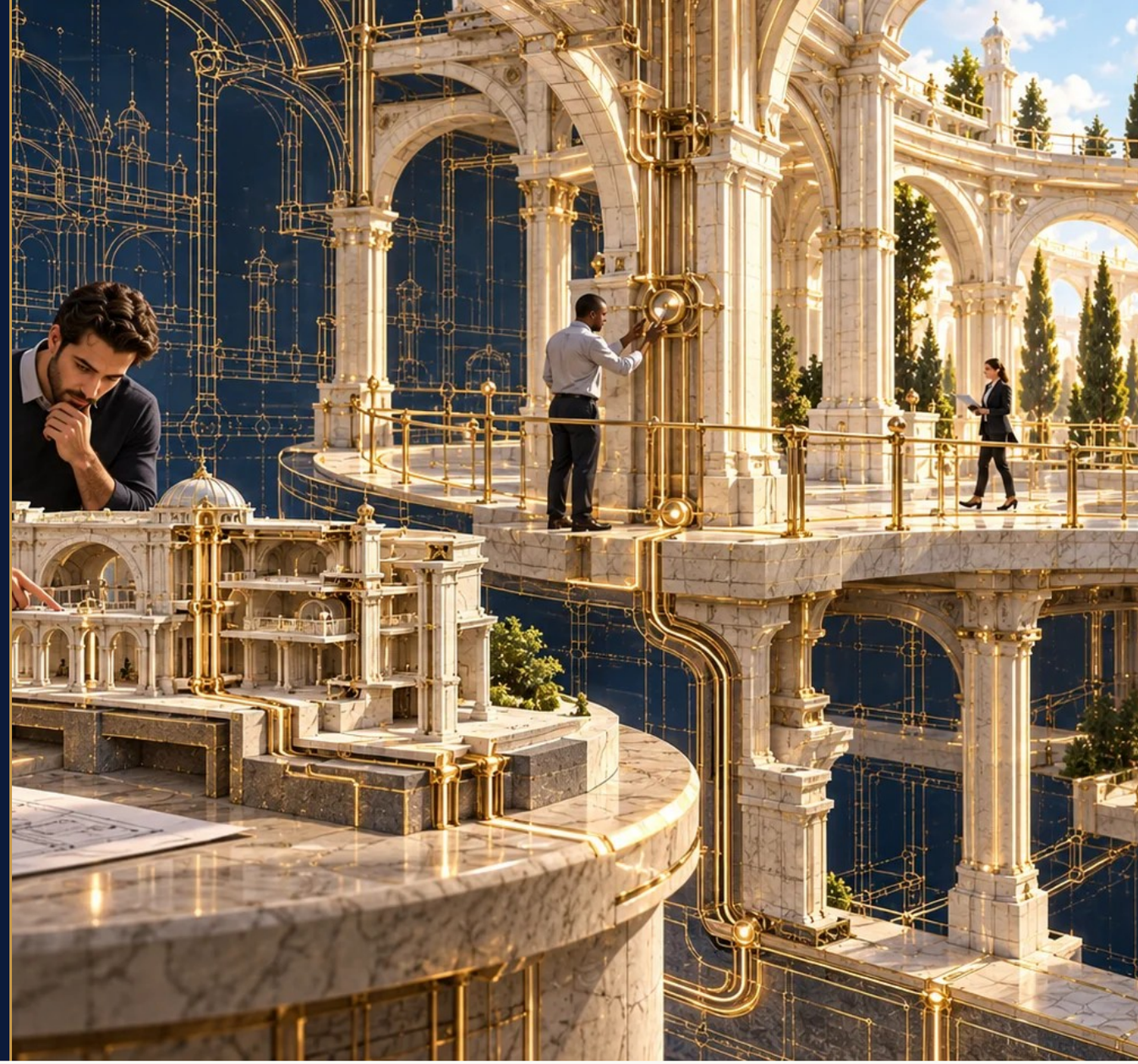
OPENAI ARCHITECTURE PRIMER

Private Safety Processing

Customer-controlled retention, protected review, and bounded signals

A visual guide to how eligible Zero Data Retention projects support offline automated safety review without OpenAI retaining customer prompts or responses.

FIRST-PARTY DOCUMENTATION / INDEPENDENT LUMINITY SYNTHESIS



The PSP control boundary

Three principles define what the protected safety workflow may retain, reveal, and use.

THREE PRINCIPLES

01 Customers control their content

Referred prompts and responses reside in customer-controlled regional storage. Customer permissions and key authorization govern access.

02 No human review

An approved hardware-attested runtime decrypts protected records for automated review. Only bounded signals and operational metadata leave in plaintext.

03 Retention serves safety only

Protected content supports approved safety purposes. OpenAI states that it cannot train models on this content or expose it to other OpenAI groups or partners.

THE OPERATING MODEL

Two linked flows

01 Request and retention

Selected interactions are protected and written to the customer storage boundary.

02 Asynchronous safety review

Approved automation retrieves protected records and releases only bounded safety decisions.

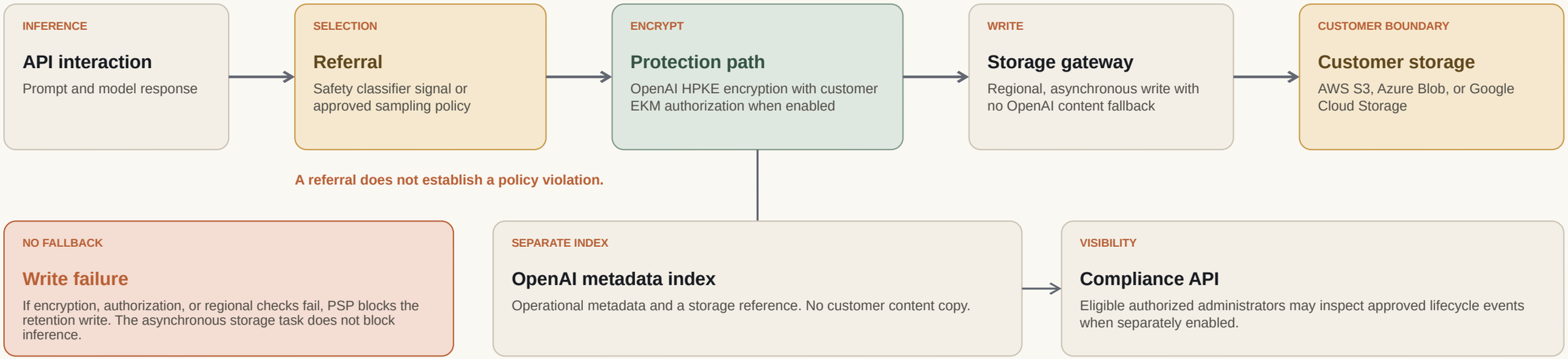
30 DAYS Customer storage minimum and OpenAI decryption window

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/private-safety-processing · verified Oct 26, 2026

API request and retention

A referred interaction is protected before it crosses into customer-controlled regional storage.



BOUNDARY OpenAI keeps routing metadata and a storage reference, not a plaintext or encrypted copy of customer content.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

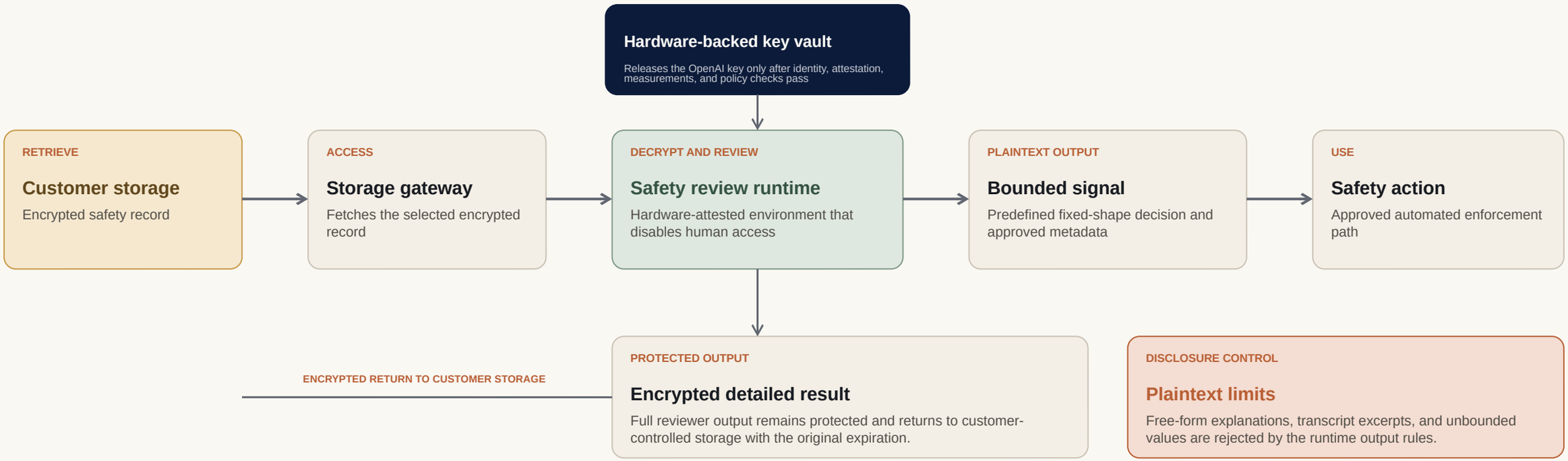
© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/private-safety-processing · verified Oct 26, 2026

OpenAI Select Partner

Asynchronous safety review

Protected records return only to an approved automated review path with bounded plaintext output.



CONTROL RULE The scheduler and storage gateway do not receive the decryption key or customer plaintext. Human access groups cannot release the key.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/private-safety-processing · verified Oct 26, 2026

OpenAI Select Partner

Project setup and operating duties

ZDR with PSP becomes active only after project storage is registered, validated, and kept healthy.

01 ZDR approval
Organization approved for Zero Data Retention

→

02 Regional storage
Dedicated AWS, Azure, or GCP destination

→

03 Register and validate
Organization administrator confirms the connection

→

04 Operate per project
PSP policy applies to all API traffic in that project

ONGOING CUSTOMER RESPONSIBILITIES

LIFECYCLE

Retain for at least 30 days

Lifecycle rules must not remove PSP records earlier. OpenAI's decryption access and metadata index expire after 30 days.

ACCESS

Maintain storage and keys

Keep regional storage, service permissions, and customer-managed key authorization correctly configured.

OPERATIONS

Monitor separate evidence

Check registration status, cloud activity logs, and Compliance API lifecycle events as distinct signals.

RESPONSE

Repair and respond

Correct unhealthy configurations and engage with OpenAI when safety concerns require investigation.

IMPORTANT Validated storage confirms a completed validation check, not continuous live connectivity. Disconnecting the last storage connection resets the project retention policy and does not delete existing cloud objects.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/private-safety-processing · verified Oct 26, 2026

OpenAI Select Partner