DATA PROCESSING AGREEMENT (DPA)
FASTWEB SERVIZI SUITE AI
(ARTICOLI 4, N. 8, E 28 DEL REGOLAMENTO UE N. 679/2016)

## Parte I - Disposizioni generali

### 1. Definizioni

1.1. I termini impiegati nel presente DPA sono definiti come i termini corrispondenti del Regolamento UE 679/2016 in materia di protezione dei dati personali (nel seguito, anche il "Regolamento"), del D. Lgs. 196/2003 aggiornato al D.Lgs. 101/2018 (nel seguito anche "Codice"), delle pertinenti norme e provvedimenti di attuazione, e del contratto stipulato con Fastweb (di seguito il "Contratto") per servizi e piattaforme di intelligenza artificiale o comunque in ambito intelligenza artificiale (di seguito "Servizi AI")
1.2. In ogni caso, i termini e le espressioni relativi alla disciplina della riservatezza sono interpretati in coerenza con il Regolamento, il Codice, le pertinenti norme e provvedimenti di attuazione e con il Contratto.

### 2. Oggetto

2.1. Il presente atto descrive gli obblighi che le parti si impegnano a rispettare per garantire un adeguato livello di protezione e rispetto delle leggi in tema di protezione dei dati personali e privacy.
Nell'ambito dell'esecuzione del Contratto e delle attività connesse (nel seguito, anche i "Trattamenti"), come definito di seguito, Fastweb S.p.A. assume il ruolo di Titolare per taluni trattamenti e di Responsabile (di seguito il "Responsabile"), ai sensi degli articoli 4, 8, e 28 del Regolamento, per conto del Cliente (di seguito Titolare ai sensi dell'articolo 4, n. 7, del Regolamento).

### 3. Ambito e finalità dei Trattamenti

3.1. I Trattamenti includono tutti i dati personali trasmessi dal Titolare o comunque raccolti o formati dal Responsabile per conto del Titolare nell'esecuzione del Contratto e delle attività connesse (si vedano i dettagli per servizio nell'Allegato 1).
3.2. Il Responsabile svolgerà i Trattamenti ai soli fini dell'esecuzione del Contratto e per quanto necessario allo stesso nonché per l'adempimento degli obblighi derivanti dal Regolamento, dalle norme e dai provvedimenti per la sua attuazione e in generale dalla legge e da provvedimenti vincolanti di Autorità pubbliche.
3.3. Il presente DPA si applica anche nelle ipotesi in cui il Cliente agisce quale Responsabile del trattamento per conto di soggetti terzi Titolari del trattamento. In tali casi Fastweb agisce quale Sub Responsabile e rimangono validi tutti gli obblighi previsti dal presente DPO in carico al Responsabile.

## Parte II - Obblighi nell'esecuzione dei Trattamenti

### 4. Garanzie nell'esecuzione dei Trattamenti

4.1. Il Responsabile svolge i Trattamenti nel rispetto del Regolamento, del Codice, delle pertinenti norme e provvedimenti di attuazione e del Contratto, ivi incluso il presente DPA.
4.2. Il Responsabile assicura che nel trattamento dei dati personali per conto del titolare rispetterà le istruzioni riportate nel presente DPA, nel Contratto nell'Allegato Tecnico e nei Termini e condizioni d'uso dei servizi, svolgendo i Trattamenti alle condizioni e nei limiti da esse previsti.
4.3. Il Responsabile garantisce il rispetto dei commi 1 e 2, e dell'articolo 3, comma 2, da parte di tutti i soggetti da esso incaricati che, a qualunque titolo, partecipano ai Trattamenti.
4.4. Il Responsabile garantisce che il personale che accede ai dati oggetto dei Trattamenti e che prende parte agli stessi sia solo quello a tal fine necessario, sia selezionato secondo requisiti di affidabilità, adeguatamente qualificato e periodicamente formato sulle garanzie nei Trattamenti, nonché tenuto sulla base di un atto tracciato al rispetto del Regolamento e delle altre norme e provvedimenti applicabili, nonché degli obblighi rilevanti derivanti dal Contratto e dal presente DPA.

### 5. Sicurezza nei Trattamenti

5.1. Il Responsabile svolge i Trattamenti con misure tecniche e organizzative che garantiscono un livello di sicurezza adeguato al rischio nei Trattamenti, secondo quanto previsto dall'articolo 32 del Regolamento, e dalle pertinenti norme e provvedimenti di attuazione. I dettagli delle misure di sicurezza tecniche sono descritti nell'Allegato 2.
5.2. Il Responsabile garantisce altresì il rispetto delle misure di sicurezza prescritte dal Titolare ai sensi dell'articolo 4.
5.3 Ciascuna parte si impegna a garantire di trattare i Dati personali ai sensi e nel rispetto delle norme e best practice in materia di privacy e protezione dei dati personali.

## 6. Registro dei Trattamenti

6.1. Il Responsabile tiene un registro dei Trattamenti nelle forme previste dall'articolo 30, paragrafi 2 e 3, del Regolamento.

## 7. Sub-affidamento dei Trattamenti ad altri responsabili

7.1. Nei limiti e alle condizioni previste dal Contratto, il Titolare rilascia al Responsabile un'autorizzazione generale al ricorso ad altri responsabili per l'esecuzione di specifiche attività che rientrino nei Trattamenti.
7.2. La lista dei sub-affidatari già designati sub responsabili del trattamento, sempre in corso di aggiornamento, è disponibile al seguente link: https://www.fastweb.it/grandi-aziende/privacy/ Sezione Sub-responsabili (Sub-processors). Tale lista viene aggiornata prima dell'affidamento dei Trattamenti ai nuovi Sub-Responsabili.
7.3. Per conoscere l'elenco dei Sub Responsabili coinvolti con riferimento allo specifico servizio, per esercitare eventuali opposizioni all'inserimento dei nuovi Sub Responsabili, o per richiedere ulteriori dettagli è disponibile il seguente indirizzo: enterprise.gdprcompetencecenter@fastweb.it . Eventuali opposizioni all'inserimento dei nuovi Sub Responsabili devono essere presentate per iscritto e corredate dalle relative motivazioni e documentazione a supporto. Fastweb si riserva la possibilità di risolvere il Contratto nel caso di opposizione all'inserimento di un nuovo Sub Responsabile.
7.4. Il Responsabile è tenuto a disciplinare il sub-affidamento con un accordo scritto vincolante conforme all'articolo 28 del Regolamento, che assicuri un livello di tutela non inferiore a quello di cui al presente DPA e comunque il rispetto dei medesimi obblighi ivi previsti per il Responsabile.

## 8. Trasferimento dei dati personali verso paesi terzi e organizzazioni internazionali

8.1. Il Responsabile, anche nell'ambito dei sub-affidamenti si cui all'articolo 7 può trasferire i dati personali oggetto dei Trattamenti verso le destinazioni di cui all'articolo 44 del Regolamento alle condizioni di cui al capo V del Regolamento, nel rispetto del presente DPA e delle istruzioni sui Trattamenti.

# Parte III - Obblighi del Responsabile di assistenza e cooperazione con il Titolare

## 9. Diritti d'informazione e di audit del Titolare

9.1. Il Responsabile è tenuto a rispondere tempestivamente alle richieste di informazioni e documentazione da parte del Titolare pertinenti ai Trattamenti.
9.2. Fastweb ha ottenuto varie certificazioni e si sottopone ad audit di terze parti. Su richiesta scritta del Titolare, e fatti salvi gli obblighi di riservatezza previsti dal Contratto, Fastweb mette a disposizione del Titolare una copia delle certificazioni.
9.3 Il Responsabile si impegna altresì a consentire al Titolare di svolgere direttamente o tramite propri incaricati, dietro richiesta formulata con preavviso di almeno 10 giorni, verifiche sulla correttezza e liceità dei trattamenti effettuati nell'ambito del Contratto, ove necessario dando anche accesso alle proprie strutture e risorse coinvolte nell'esecuzione del Contratto e nei Trattamenti, in forme compatibili con lo svolgimento delle attività aziendali del Responsabile.

## 10. Doveri di cooperazione del Responsabile

10.1. Il Responsabile, in relazione ai Trattamenti affidatigli, assiste il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a sua disposizione e in conformità alle istruzioni fornite dal Titolare ai sensi dell'articolo 4.

## 11. Diritti degli interessati

11.1. Il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento, anche in conformità alle istruzioni fornite dal Titolare ai sensi dell'articolo 4.
11.2. Il Responsabile informa tempestivamente il Titolare di ogni richiesta di esercizio dei diritti di cui al capo III del Regolamento, rivolta a lui o a sub-responsabili da lui designati con riferimento ai Trattamenti, e coopera con il Titolare per la definizione delle risposte a tali richieste.

## 12. Violazioni dei dati personali

12.1. Salvo quanto previsto dagli articoli 9, 10 e 13, il Responsabile si impegna a comunicare al Titolare ai contatti forniti in fase contrattuale, senza ingiustificato ritardo dall'avvenuta conoscenza, ogni violazione dei dati personali ai sensi del Regolamento e delle pertinenti norme e provvedimenti di attuazione.
12.2. Fastweb in qualità di Responsabile del trattamento potrà comunicare al Titolare, ai sensi dell'art. 33 par. 2 GDPR, le sole possibili violazioni di dati personali di cui viene o può venire a conoscenza nei propri sistemi strumentali alla fornitura dei servizi di cui al Contratto.
12.3. La comunicazione di cui al comma 1 contiene tutti gli elementi necessari al Titolare per adempiere agli obblighi in tema di violazione dei dati personali nonché per intervenire e porre rimedio alla violazione o mitigare i suoi effetti. La comunicazione, in ogni caso, indica i dati, le categorie e il numero degli interessati, la violazione circostanziata, le conseguenze attuali e potenziali, le misure prese in risposta.
12.4. Il Responsabile è in ogni caso tenuto a svolgere senza indugio le azioni necessarie per individuare con precisione gli eventi e mitigare o rimuovere le loro conseguenze, riducendo al minimo gli eventuali danni, anche cooperando con il Titolare.
12.5 In ogni caso, nessuna notifica di incidente sui dati effettuata al Titolare potrà essere considerata quali riconoscimento da parte del Responsabile di qualsiasi colpa o responsabilità in relazione all'incidente di dati.

## 13. Rapporti con le Autorità

13.1. Il Responsabile risponde tempestivamente alle richieste di informazione e di documentazione rivolte, nell'esercizio delle loro funzioni, dal Garante per la protezione dei dati personali e dalle altre Autorità di controllo competenti per la protezione dei dati personali.

# Parte IV - Disposizioni finali

## 14. Comunicazioni

14.1. Tutte le comunicazioni afferenti all'esecuzione del presente DPA vengono svolte, ove non diversamente indicato dall'DPA medesimo, ai punti di contatto indicati dal Contratto.

## 15. Modifiche del DPA

15.1. Fermo quanto previsto dai precedenti articoli, il Responsabile può aggiornare e apportare variazioni al presente DPA che siano ragionevolmente necessarie per adempiere agli obblighi derivanti dal Regolamento e dalle altre norme in materia di dati personali o per tenere conto delle clausole tipo e dei codici di condotta eventualmente adottati ai sensi, rispettivamente, dell'articolo 28, paragrafi 7 e 8, e dell'articolo 40 del Regolamento o ai fini delle certificazioni di cui all'articolo 42 del Regolamento.
15.2. Le versioni aggiornate del DPA sono pubblicate sul sito del Responsabile (https://www.fastweb.it/grandi-aziende/privacy/). Il DPA aggiornato sarà efficace non appena pubblicato sul sito o secondo quanto diversamente previsto nel Contratto.

## 16. Durata e adempimenti conseguenti alla cessazione del Contratto

16.1. L'affidamento dei Trattamenti al Responsabile ha la medesima durata prevista dal Contratto.
Il presente DPA rimane in vigore fino all'effettivo perfezionamento di quanto previsto dall'art. 16.3.
16.2. Il decorso del termine finale di durata del Contratto o comunque la cessazione del Contratto e dell'efficacia del presente DPA non esentano il Responsabile dal rispetto degli obblighi che per loro natura devono continuare anche dopo la cessazione.

16.3. In tutti i casi di cessazione del Contratto e dell'efficacia del DPA, il Responsabile si obbliga, a scelta del Titolare, a cancellare i dati personali in suo possesso per l'esecuzione del Contratto e oggetto dei Trattamenti o a restituire al Titolare tali dati e cancellare le copie esistenti, salvi gli obblighi legali di conservazione.
16.4. Nell'ambito degli obblighi di cui ai commi 2 e 3, il Responsabile deve comunque attenersi al divieto di comunicazione e di diffusione dei dati personali, tranne nel caso in cui tali trattamenti siano oggetto di istruzioni documentate del Titolare e deve altresì adottare misure per minimizzare il trattamento dei dati personali in relazione agli scopi legittimamente perseguibili.

*  *  *

**Allegato 1**
**Scheda trattamento Servizi SUITE AI**

| Servizio | Tipologia di dati personali | Tipologia di interessati | Misure di sicurezza |
|---|---|---|---|
| **FastwebAI Work** | • Identificativi: indirizzo e-mail, username e password<br>• log su attività in Piattaforma,<br>• qualsiasi altro dato personale inserito nella Piattaforma dagli utenti | • Utenti della Piattaforma (SuperAdmin, Admin e Utenti Base)<br>• qualsiasi persona fisica a cui si riferiscono i dati personali eventualmente caricati all'interno della Piattaforma Fastweb AI Work dagli Utenti. | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |
| **FastwebAI Agents** | • Identificativi: indirizzo e-mail, username e password<br>• log su attività in Piattaforma,<br>• qualsiasi altro dato personale inserito nella Piattaforma dagli utenti | • Utenti della Piattaforma (Amministratore organizzazione, Amministratore workspace, Utenti Base)<br>• qualsiasi persona fisica a cui si riferiscono i dati personali eventualmente caricati all'interno della Piattaforma Fastweb AI Agents dagli Utenti. | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |
| **FastwebAI Factory** | Tenuto conto delle peculiarità del Servizio nonché | Persone fisiche, tra cui ad esempio dipendenti, clienti, | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico |

| | | | |
|---|---|---|---|
| | del settore di attività del Titolare i trattamenti potrebbero riguardare le tipologie di dati personali (es. dati comuni, dati particolari ex art. 9 del Regolamento ecc..) affidati dal Titolare al Responsabile nel corso dell'erogazione del Servizio. | leads, prospect, utenti, fornitori del Titolare nonché qualsiasi persona fisica a cui si riferiscono i dati personali affidati dal Titolare al Responsabile nel corso dell'erogazione del Servizio. | definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |
| **FastwebAI Custom** | Tenuto conto delle peculiarità del Servizio nonché del settore di attività del Titolare i trattamenti potrebbero riguardare le tipologie di dati personali (es. dati comuni, dati particolari ex art. 9 del Regolamento ecc..) affidati dal Titolare al Responsabile nel corso dell'erogazione del Servizio. | Persone fisiche, tra cui ad esempio dipendenti, clienti, leads, prospect, utenti, fornitori del Titolare nonché qualsiasi persona fisica a cui si riferiscono i dati personali affidati dal Titolare al Responsabile nel corso dell'erogazione del Servizio. | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |
| **FastwebAI G&C** | • Identificativi: indirizzo e-mail, username e password<br>• log su attività in Piattaforma,<br>• qualsiasi altro dato personale inserito nella Piattaforma dagli utenti | • Utenti della Piattaforma (Admin e Utenti Base)<br>• qualsiasi persona fisica a cui si riferiscono i dati personali eventualmente caricati all'interno della Piattaforma dagli Utenti. | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |
| **Fine tuning Modello** | Tenuto conto delle peculiarità del Servizio nonché del settore di attività del Titolare | • qualsiasi persona fisica a cui si riferiscono i dati personali eventualmente | Con riferimento alle misure tecniche e organizzative si veda l'Allegato Tecnico definito con il singolo cliente, nonché l'Allegato 2 del presente DPA. |

| | | | |
|---|---|---|---|
| | i trattamenti potrebbero riguardare tutte le tipologie di dati personali (es. dati comuni, dati particolari ex art. 9 del Regolamento, dati relativi a condanne penali e reati ex art. 10 del Regolamento, ecc.) contenuti nei Materiali del Cliente che il Titolare mette a disposizione del Responsabile per le attività di ine tuning del Modello | contenuti nei Materiali del Cliente | |

## Allegato 2
## Misure di sicurezza

Si riportano di seguito le misure di sicurezza dell'infrastruttura di Fastweb per l'erogazione di servizi di Intelligenza Artificiale, nonché le misure delle singole soluzioni AI di Fastweb.

### Fastweb AI Factory

- È situato in un Data Center (DC) nel nord Italia, Tier IV, protetto da un sistema di sicurezza fisica multilivello.
- La sua architettura è stata specificamente progettata per supportare e facilitare l'espansione futura, garantendo così la scalabilità dell'infrastruttura
- Architettura segregata che assicura che i dati e i processi di ciascun cliente rimangano isolati e protetti, prevenendo accessi non autorizzati e garantendo la conformità con i più rigorosi standard di sicurezza informatica.
- La protezione dell'infrastruttura è garantita da apparati F5 e da altri fornitori top di gamma che implementano meccanismi di controllo accessi, protezione da attacchi DDoS e cyber, e sicurezza specifica per l'inferenza di modelli LLM.

### FASTEDGE

- FastEdge è utilizzata per gestire workload tradizionali e di AI non generativa.
- Questa infrastruttura è distribuita su diversi Data Center dislocati sul territorio italiano.
- FastEdge è connessa con il FastwebAI Factory tramite una rete ad alta velocità, per garantire comunicazione efficiente e a bassa latenza.
- FastEdge è utilizzata anche per ospitare i backup dell'infrastruttura AI con storage ECS da 5 PB.
- La sicurezza complessiva delle infrastrutture FastwebAI Factory e FastEdge è verificata periodicamente da un operatore specializzato in cyber security (7Layers).

### Fastweb AI Work

- Logging

- Autenticazione e autorizzazione
- Autenticazione a due fattori (2fa) opzionale
- Crittografia dei dati at-rest e in-transit
- Localizzazione dei dati in data center situati in Europa

**Fastweb AI Agent**

- Politiche di data retention per dati di monitoraggio su applicativo
- Politiche di visibilità della Organizzazione cliente verso Fastweb
- Backup giornalieri con retention di cinque giorni
- Role-based access control

**Fastweb AI G&C**

- Logging
- Autenticazione e Autorizzazione
- Autenticazione a due fattori (2fa) opzionale
- Crittografia dei dati at-rest e in-transit
- Localizzazione dei dati (in caso di accesso Piano Premium e Standard modalità SaaS) in data center situati in Europa
- Log conservati per 6 mesi (in caso di accesso SaaS), per la rilevazione di anomalie e troubleshooting

Le soluzioni AI di Fastweb integrano i Modelli di terze parti per il tramite di fornitori di servizi cloud gestiti per l'accesso e l'utilizzo di modelli di AI che sono qualificati come sub-Responsabili del trattamento.

Si riportano di seguito le principali misure di sicurezza delle soluzioni che permettono l'integrazione tra i Modelli di terze parti e le soluzioni AI di Fastweb. Per una descrizione più dettagliata si faccia riferimento alle informazioni contenute nei link riportati.

**Servizio Vertex AI Web Grounding for Enterprise**

- **Riservatezza**
  Google non usa i Customer Data per addestrare o per svolgere attività di fine-tuning dei modelli AI/ML senza previa autorizzazione o istruzione del cliente.
  Per i Fine-Tuned Google Models e i Google Customer-Trained Models, il cliente ha accesso esclusivo e né Google né terzi non autorizzati dal cliente possono accedervi o usarli, anche dopo la cessazione del contratto.
  Per i Generative AI Services, in assenza di previa autorizzazione o istruzione del cliente, Google non conserva fuori dall'account del cliente:
  1. i prompt / Customer Data più a lungo di quanto ragionevolmente necessario per generare l'output;
  2. il Generated Output stesso.
- **Crittografia:** Utilizzo di Customer-Managed Encryption Keys (CMEK)
- **Access Transparency e Data Residency** funzionali anche a verificabilità, auditabilità e accountability;
- **Controlli di fine-grained access control** per le operazioni generative AI, utili a supportare revisione, governance e verifica periodica delle autorizzazioni.

Per ulteriori dettagli sulle misure di sicurezza di Vertex AI si rimanda ai termini e condizioni e alle misure di sicurezza descritte nei seguenti link:
https://cloud.google.com/terms/service-terms

Cloud Data Processing Addendum | Google Cloud
https://services.google.com/fh/files/misc/
genai_privacy_google_cloud_202308.pdf

## Servizio Bedrock di Amazon

- **Riservatezza:**
  - i prompt e gli output non sono messi a disposizione dei provider terzi dei modelli;
  - AWS e i provider terzi non usano input e output di Bedrock per addestrare Amazon Nova, Amazon Titan o modelli di terzi;
  - il modello customizzato resta ad uso esclusivo del cliente e i provider terzi non possono accedervi;
  - AWS non accederà né userà il modello customizzato se non per erogare/manutenere il servizio o per obbligo di legge/ordine vincolante dell'autorità.
- il **controllo degli accessi** può essere rafforzato tramite IAM e connettività privata tramite AWS PrivateLink, evitando l'esposizione del traffico su Internet pubblico.
- **Bedrock Guardrails**, con filtri per contenuti dannosi, denied topics, word filters e filtri per informazioni sensibili:
  - **protezione** contro prompt attacks, inclusi jailbreak, prompt injection e, nello standard tier, prompt leakage;
  - **contextual grounding checks** per ridurre risposte non fondate o allucinazioni;
  - **automated reasoning checks** per rilevare inesattezze fattuali, suggerire correzioni e spiegare perché una risposta è o non è valida;
- **Cifratura:** Amazon Bedrock prevede che i dati siano encrypted in transit and at rest e consente anche la gestione delle chiavi tramite AWS KMS, inclusa la possibilità di usare chiavi controllate dal cliente. In aggiunta, durante il fine-tuning o la customizzazione privata del modello, i dati non lasciano la rete AWS; transitano in modo sicuro attraverso la VPC del cliente;
- Bedrock è incluso in framework di **audit e compliance come SOC, ISO, CSA STAR Level** 2, oltre a essere indicato come utilizzabile in conformità al GDPR;
- extensive third-party audits dei controlli AWS;
- **monitoring e logging tramite CloudWatch e CloudTrail**, con possibilità di conservare metadati, richieste e risposte in S3 e CloudWatch Logs, utili per audit, verifica e troubleshooting

  Per ulteriori dettagli sulle misure di sicurezza di Bedrock di Amazon si rimanda ai termini e condizioni e alle misure di sicurezza descritte nei seguenti link:
  - https://aws.amazon.com/service-terms/
  - https://aws.amazon.com/bedrock/faqs/
  - https://aws.amazon.com/bedrock/security-compliance/

## Azure Open AI

- **Riservatezza:**
  - Azure OpenAI non usa i dati del cliente per riaddestrare i modelli
  - I Customer Data, Prompts e Completions non sono usati per migliorare prodotti o servizi Microsoft o di terzi senza esplicito permesso o istruzione del cliente.
  - I dati non sono resi disponibili a OpenAI o ad altri model provider e i modelli Azure Direct sono eseguiti nell'ambiente Azure di Microsoft, senza interazione con servizi operati da OpenAI come ChatGPT o OpenAI API.
  - Quando vengono usate alcune funzionalità opzionali, come Responses API, Threads o Stored completions, il servizio crea un data store persistente; tale archivio è collocato nella geografia Azure in cui è distribuita la risorsa del cliente.
  - I prompt e i contenuti generati vengono conservati nella Azure geography di deployment della risorsa, all'interno del service boundary del servizio.

- **Criptazione:** Cifratura a riposo con customer-managed keys per i contenuti del cliente conservati dal servizio. Il servizio supporta data at-rest encryption using customer-managed keys, oltre all'integrazione nativa con Azure Key Vault per la gestione di credenziali. Inoltre, per alcuni componenti enterprise collegati alle soluzioni generative, vi è anche il supporto a CMEK;
- **Controllo degli accessi:**
  - supporto a Azure AD authentication per l'accesso data plane;
  - supporto a Azure RBAC per la gestione degli accessi alle azioni sul data plane;
  - disponibilità di Customer Lockbox, per consentire al cliente di approvare o rifiutare richieste di accesso ai dati da parte di Microsoft in scenari di supporto
- **Sicurezza di rete:**
  - Microsoft permette di configurare **network isolation end-to-end** tramite **Private Link**, per proteggere la comunicazione con le risorse Foundry / Azure AI.
  - La security baseline Azure OpenAI richiama inoltre controlli di **data loss prevention** che consentono di configurare l'elenco degli **outbound URLs** autorizzati per le risorse Azure OpenAI
- **content filtering** e **abuse monitoring** come meccanismi integrati di prevenzione del misuse.
- Microsoft Foundry mette a disposizione un **Risks & Safety monitoring dashboard** per i deployment che usano un content filter, così da verificare l'attività di filtraggio e i risultati dei controlli di sicurezza.
- Per le funzionalità di **potentially abusive user detection**, Microsoft supporta anche l'opzione **bring your own storage**, così che gli insight dettagliati siano conservati in modo controllato e conforme dal cliente.
- **Access Transparency**

Per ulteriori dettagli sulle misure di sicurezza di Azure Open AI si rimanda ai termini e condizioni e alle misure di sicurezza descritte nei seguenti link:
https://learn.microsoft.com/it-it/security/benchmark/azure/baselines/azure-openai-security-baseline
Criteri di protezione predefiniti per Azure OpenAI - Microsoft Foundry | Microsoft Learn