

Versione di lancio 2026-08-03. Documento di riferimento pubblicato ai fini dell'ordine: in caso di sottoscrizione fa fede la copia firmata digitalmente e scambiata via PEC. Fornitore: BLAPP S.r.l., [sede legale e P.IVA — in aggiornamento] · sante.stanisci@blapp.it

Accordo sul trattamento dei dati personali (DPA)

Ai sensi dell'art. 28 del Regolamento (UE) 2016/679 ("GDPR"). Allegato alle Condizioni Generali di Servizio e al contratto di abbonamento AYD.

1. Ruoli e oggetto

1.1 Il Cliente è **Titolare** del trattamento dei dati personali contenuti nei documenti caricati e nei dati degli utenti da lui creati; **BLAPP S.r.l.** è **Responsabile** del trattamento ex art. 28 GDPR.

1.2 Il presente accordo disciplina il trattamento svolto dal Responsabile per conto del Titolare nell'ambito del servizio AYD.

2. Natura, finalità e durata

- **Natura e finalità:** conservazione dei documenti, estrazione del testo, indicizzazione semantica, ricerca e generazione di risposte a beneficio esclusivo del Titolare; log tecnici e di utilizzo per sicurezza e fatturazione.
- **Durata:** per tutta la durata del servizio e fino alla cancellazione di cui all'art. 7.
- **Categorie di dati e interessati:** definite dal Titolare tramite i documenti caricati (tipicamente dati di dipendenti, clienti e fornitori del Titolare). Il Titolare si impegna a non caricare categorie particolari di dati ex art. 9 GDPR salvo accordo scritto.

3. Obblighi del Responsabile

Il Responsabile: tratta i dati solo su istruzione documentata del Titolare (l'uso del servizio costituisce istruzione); garantisce che le persone autorizzate siano vincolate alla riservatezza; **non usa i dati per finalità proprie né per addestrare modelli**; assiste il Titolare nelle risposte agli interessati e negli obblighi ex artt. 32–36 GDPR.

4. Misure di sicurezza (art. 32)

- Isolamento logico dei dati per cliente a livello di database (Row Level Security) e di storage.
- Cifratura at-rest applicativa AES-256-GCM dei documenti originali e dei testi indicizzati (gli embedding vettoriali restano in chiaro per necessità tecnica della ricerca).
- Classificazione dei documenti su 4 livelli di sensibilità con autorizzazioni per utente, applicate dalle policy del database.
- Impronta di integrità SHA-256 per ogni documento; tracciamento delle operazioni nei log di servizio.
- Cifratura in transito (TLS); credenziali con hash; accesso amministrativo limitato e tramite chiavi.
- Backup periodici cifrati; registro dei trattamenti e log tecnici con rotazione.

5. Sub-responsabili

5.1 Il Titolare autorizza in via generale il ricorso a sub-responsabili; il Responsabile ne mantiene l'elenco aggiornato e comunica le modifiche con 15 giorni di preavviso, entro i quali il Titolare può opporsi per motivi legittimi.

5.2 Elenco attuale:

Sub-responsabile	Attività	Ubicazione
OVHcloud (OVH Groupe SAS / OVH Italia)	Infrastruttura server e servizio di inferenza AI (AI Endpoints)	Datacenter UE

5.3 Il servizio di inferenza riceve, per la sola elaborazione della risposta, gli estratti di testo pertinenti alla domanda; secondo i termini del fornitore i dati non sono conservati né usati per addestramento.

6. Violazioni di dati (data breach)

Il Responsabile notifica al Titolare senza ingiustificato ritardo, e comunque entro **72 ore** da quando ne ha avuto conoscenza, ogni violazione di dati personali, fornendo le informazioni utili ex art. 33 GDPR.

7. Cancellazione e restituzione

Alla cessazione del servizio, o su richiesta del Titolare, il Responsabile cancella documenti, indici e dati personali (salvo obblighi di legge) entro 30 giorni, dandone conferma scritta. Su richiesta, prima della cancellazione, restituisce i documenti originali.

8. Audit

Il Responsabile mette a disposizione le informazioni necessarie a dimostrare la conformità e consente audit del Titolare, con preavviso di almeno 15 giorni, al massimo una volta l'anno salvo violazioni, a spese del Titolare.

9. Trasferimenti extra-UE

Non sono previsti trasferimenti di dati verso paesi terzi. Ogni eventuale futuro trasferimento sarà preventivamente concordato e assistito da garanzie adeguate (Capo V GDPR).