Informativa sul trattamento dei dati personali — AYD

Versione: privacy-2026-08-03 (sostituisce privacy-2026-07-29) · Informativa resa ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679 ("GDPR").

1. Che cos'è AYD e a chi si rivolge questa informativa

AYD è un servizio software per aziende (B2B) di BLAPP S.r.l.: l'azienda cliente carica i propri documenti e il proprio team può porre domande in linguaggio naturale sul loro contenuto. Questa informativa riguarda:

- le persone che si registrano e usano AYD (account amministratore e membri del team);
- i visitatori del sito di AYD;
- le persone i cui dati personali compaiono nei documenti caricati dalle aziende clienti (per questa parte, si veda la sezione 2 sul nostro ruolo di responsabile del trattamento).

2. Titolare del trattamento e i nostri due ruoli

Il titolare del trattamento è **BLAPP S.r.l.**, [sede legale e P.IVA — in aggiornamento]. Per qualsiasi richiesta relativa ai dati personali: **sante.stanisci@blapp.it**.
BLAPP riveste due ruoli distinti, ed è importante capire la differenza:

- **Titolare del trattamento** per i dati che raccogliamo direttamente per far funzionare il servizio: dati di account (email, password, ruolo), dati dell'azienda cliente, registrazioni dell'accettazione di questa informativa, log di utilizzo e log tecnici del sito.
- **Responsabile del trattamento** (art. 28 GDPR) per il **contenuto dei documenti** che le aziende clienti caricano. Di quei contenuti — che possono includere qualsiasi categoria di dato personale, anche dati particolari ex art. 9 GDPR — il titolare è l'azienda cliente, che decide cosa caricare e perché. Trattiamo quei contenuti solo per fornire il servizio (indicizzazione e risposta alle domande). Per i piani a pagamento questo trattamento è disciplinato da un accordo sul trattamento dei dati (DPA) ex art. 28 GDPR, parte del contratto; per il piano di prova gratuito, le istruzioni e le condizioni del trattamento sono quelle descritte in questa informativa. Se i tuoi dati compaiono in documenti caricati da una nostra azienda cliente, il tuo referente per l'esercizio dei diritti è quell'azienda; noi forniremo al cliente la collaborazione necessaria.

3. Quali dati trattiamo, perché e per quanto tempo

Categoria di dati	Finalità	Base giuridica	Conservazione
Dati di account: nome azienda, email aziendale, password (conservata solo come hash bcrypt, mai in chiaro), ruolo e livello di autorizzazione	Registrazione, autenticazione, gestione del team, controllo degli accessi per livello di sensibilità	Esecuzione del contratto (art. 6.1.b GDPR)	Per tutta la durata dell'account; eliminati con la chiusura dell'account
Dati dell'azienda cliente: ragione sociale, piano sottoscritto, dominio email aziendale	Identificazione del cliente, applicazione dei limiti di piano, vincolo di dominio per i membri del team	Esecuzione del contratto (art. 6.1.b GDPR)	Per tutta la durata del rapporto contrattuale
Registrazione dell'accettazione di questa informativa: versione accettata e data/ora	Prova dell'accettazione dell'informativa (responsabilizzazione)	Legittimo interesse (art. 6.1.f GDPR)	Per tutta la durata dell'account
Documenti caricati (PDF, DOCX, TXT, MD, max 20 MB) e testi estratti per l'indicizzazione, con nome file, impronta di integrità (SHA-256) e livello di sensibilità	Fornitura del servizio: indicizzazione dei contenuti e risposta alle domande del team	Definita dal cliente titolare del contenuto (BLAPP agisce come responsabile ex art. 28)	Fino alla cancellazione del documento da parte del cliente o alla chiusura dell'account
Rappresentazioni vettoriali dei testi (embeddings)	Ricerca semantica: individuare i passaggi pertinenti alla domanda	Come sopra (dato derivato dai documenti)	Eliminati automaticamente insieme al documento da cui derivano
Log di utilizzo: tipo di operazione (caricamento, cancellazione, domanda), modello usato, conteggio token, durata, data/ora, identificativo utente. **Il testo**	Applicazione dei limiti di piano, misura dei consumi	Esecuzione del contratto e legittimo interesse (art. 6.1.b e 6.1.f GDPR)	Massimo 12 mesi (v. sezione 8)

Categoria di dati	Finalità	Base giuridica	Conservazione
delle domande non viene registrato.			
Log tecnici del server web: indirizzo IP, data/ora, risorsa richiesta, pagina di provenienza (referer), user-agent	Sicurezza e diagnostica del servizio	Legittimo interesse (art. 6.1.f GDPR)	Massimo 12 mesi (v. sezione 8)
Token di sessione (conservato nel browser dell'utente)	Mantenere attiva la sessione di lavoro	Esecuzione del contratto (art. 6.1.b GDPR)	Validità massima 7 giorni; rimosso dal dispositivo al logout o cancellando i dati del browser

3.1 Precisazioni sui dati di account

- Richiediamo **email aziendali**: gli indirizzi dei più comuni provider gratuiti/personali vengono rifiutati alla registrazione. Un'email aziendale nominativa (es. nome.cognome@azienda.it) resta comunque un dato personale e la trattiamo come tale.
- La password non è mai conservata in chiaro (hash bcrypt con salt). **Non esiste al momento un recupero password automatico**: in caso di smarrimento, scrivi a sante.stanisci@blapp.it e gestiremo la richiesta manualmente, previa verifica dell'identità.
- Gli account dei membri del team sono creati dall'amministratore dell'azienda cliente, con email appartenenti al dominio aziendale. **Ogni membro del team accetta questa informativa al primo accesso all'applicazione**: registriamo versione e data dell'accettazione. Resta buona prassi che chi amministra l'account la porti a conoscenza del team già al momento della creazione degli accessi.
- L'elenco degli utenti di un'azienda (email, ruolo, livello di autorizzazione, data di creazione) è visibile solo all'amministratore di quell'azienda.

3.2 Precisazioni sui documenti caricati

- Ogni documento e ogni passaggio indicizzato ha un livello di sensibilità (pubblico, interno, riservato, ristretto): solo gli utenti con autorizzazione sufficiente possono vederlo, caricarlo o cancellarlo. Il controllo è applicato a livello di database.

- **Il nome del file è conservato in chiaro** (nel database e nello storage), a differenza del contenuto, che è cifrato. Consigliamo di non inserire dati personali nei nomi dei file (es. evitare "CV Mario Rossi.pdf").
- Di ogni file conserviamo un'impronta crittografica (SHA-256) che ne fissa il contenuto al momento del caricamento.
- Ogni azienda cliente è responsabile della liceità dei contenuti che carica e delle informative rese ai propri interessati.

3.3 Precisazioni sugli embeddings

Gli embeddings sono rappresentazioni numeriche dei testi, calcolate **interamente sui nostri server** (nessun dato viene inviato all'esterno per l'indicizzazione). Per necessità tecnica non sono cifrati: la ricerca semantica deve poter operare direttamente sui vettori. Poiché dalla letteratura scientifica risulta possibile una ricostruzione parziale del testo di origine, li trattiamo come dati personali ogni volta che il testo di origine lo è, e li proteggiamo con le stesse misure di isolamento e controllo accessi dei documenti.

4. Il flusso verso il fornitore di intelligenza artificiale (OVH AI Endpoints)

Questo è l'**unico caso** in cui contenuti dei documenti lasciano i nostri server, e vogliamo descriverlo con precisione.

- Quando un utente pone una domanda e il modello linguistico è attivo, inviamo al servizio OVH AI Endpoints: la **domanda** dell'utente, i **passaggi più pertinenti** dei documenti (al massimo 5 estratti, decifrati per l'occasione) e i **nomi dei file** da cui provengono.
- **Non** inviamo: l'intero archivio documentale, gli embeddings, gli identificativi dell'azienda o dell'utente, gli indirizzi email.
- Se il modello linguistico non è configurato, il servizio funziona in sola modalità di ricerca e **nessun dato esce dai nostri server**.
- AYD **non conserva** le domande poste né le risposte generate; registriamo solo dati tecnici di consumo (conteggio token, durata).
- Noi non utilizziamo i contenuti dei clienti per addestrare modelli di intelligenza artificiale. OVH agisce come sub-responsabile del trattamento; le condizioni applicabili al suo trattamento sono definite nel rapporto contrattuale con OVH.

5. Trasparenza sull'uso dell'IA (art. 50 Regolamento UE 2024/1689 — AI Act)

- Le risposte alle domande sono **generate da un sistema di intelligenza artificiale** (un modello linguistico di grandi dimensioni), sulla base dei passaggi pertinenti estratti dai documenti dell'azienda.
- Le risposte possono contenere imprecisioni o errori: il sistema cita gli estratti utilizzati proprio per consentirne la verifica. Le informazioni rilevanti vanno sempre riscontrate sui documenti originali.
- AYD non adotta decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici o incidano in modo analogo significativo sulle persone (art. 22 GDPR).

6. Destinatari, sub-responsabili e trasferimenti

- Non vendiamo né cediamo dati personali a terzi. Il sito e l'applicazione **non contengono strumenti di analytics, pixel o traccianti di terze parti**.
- I dati sono trattati su server **OVH** in un datacenter nell'Unione Europea, secondo quanto dichiarato dal fornitore.
- Sub-responsabili del trattamento: **OVH** (hosting dell'infrastruttura) e **OVH AI Endpoints** (elaborazione delle domande e degli estratti pertinenti, come descritto alla sezione 4). L'elenco aggiornato dei sub-responsabili è disponibile su richiesta.
- Non è previsto alcun trasferimento di dati personali al di fuori dell'Unione Europea.

7. Misure di sicurezza

Misure effettivamente in essere:

- connessioni al servizio su canale cifrato (HTTPS/TLS);
- **cifratura a riposo AES-256-GCM** dei documenti originali (cifrati prima di toccare lo storage) e dei testi indicizzati (cifrati prima del salvataggio nel database);
- password protette con hash bcrypt e salt;
- **isolamento tra aziende clienti** applicato a livello di database (Row Level Security in modalità fail-closed): gli utenti di un'azienda non possono accedere ai dati di un'altra;
- controllo degli accessi per livello di sensibilità (4 livelli), applicato anch'esso a livello di database;
- impronta crittografica SHA-256 di ogni file, registrata al caricamento.

Per trasparenza, segnaliamo anche i limiti attuali e i nostri impegni:

- la cifratura a riposo copre documenti e testi indicizzati, **non la totalità dei dati**: embeddings, nomi dei file, email degli account e log non sono cifrati a livello applicativo;
- la gestione della chiave di cifratura è oggi essenziale (chiave conservata sul server); ci impegniamo a rafforzarla nel tempo;
- eseguiamo **backup periodici cifrati**; sono conservati nella stessa infrastruttura del servizio (la ridondanza geografica è in programma), quindi resta buona norma conservare anche gli originali dei file che carichi;
- la sessione di lavoro dura al massimo 7 giorni e il logout la rimuove dal dispositivo, ma **non esiste oggi una revoca centralizzata delle sessioni**: proteggi il dispositivo da cui accedi.

In caso di violazione dei dati personali, adempiremo agli obblighi di notifica al Garante e, ove richiesto, agli interessati (artt. 33-34 GDPR).

8. Conservazione e cancellazione

- **Documenti**: cancellabili in autonomia dall'applicazione, in ogni momento, da un utente con autorizzazione sufficiente. La cancellazione elimina immediatamente il documento, i testi indicizzati e gli embeddings dal database e rimuove il file cifrato dallo storage.
- **Membri del team**: l'amministratore può eliminare gli account dei membri del proprio team dall'applicazione. Alla cancellazione di un utente, i suoi log di utilizzo vengono contestualmente anonimizzati: l'identificativo dell'utente viene rimosso.
- **Account e dati dell'azienda**: la cancellazione dell'intero account **non è al momento disponibile in autonomia dall'applicazione**. Va richiesta scrivendo a sante.stanisci@blapp.it; provvederemo manualmente alla cancellazione di account, utenti, documenti, testi indicizzati, embeddings e file in storage entro 30 giorni dalla richiesta.
- **Log di utilizzo e log tecnici**: i log di utilizzo vengono eliminati automaticamente dopo 12 mesi; i log tecnici sono soggetti a rotazione automatica che ne limita la conservazione.

9. Cookie e archiviazione locale

AYD **non usa cookie**, né di prima né di terza parte, e non usa strumenti di profilazione o analytics. L'unico dato salvato sul tuo dispositivo è il token di sessione, conservato nella memoria locale del browser (localStorage): è strettamente necessario al funzionamento del servizio, viene rimosso al logout e perde comunque validità dopo 7 giorni. Puoi eliminarlo in ogni momento cancellando i dati di navigazione del browser.

10. I tuoi diritti

Ai sensi degli artt. 15-22 GDPR puoi esercitare, nei limiti previsti dalla legge, i diritti di:

- accesso ai tuoi dati personali (art. 15);
- rettifica (art. 16);
- cancellazione (art. 17);
- limitazione del trattamento (art. 18);
- portabilità dei dati (art. 20);
- opposizione al trattamento basato sul legittimo interesse (art. 21).

Per esercitarli scrivi a **sante.stanisci@blapp.it**: risponderemo entro un mese dalla richiesta. Se i tuoi dati compaiono in documenti caricati da una nostra azienda cliente, il titolare di quel trattamento è l'azienda cliente: rivolgi a lei la richiesta; noi le forniremo il supporto tecnico necessario (ricerca, cancellazione). Hai inoltre il diritto di proporre reclamo al **Garante per la protezione dei dati personali** (www.garanteprivacy.it) o all'autorità di controllo del Paese UE in cui risiedi o lavori.

11. Servizio B2B e minori

AYD è un servizio riservato ad aziende e professionisti: non è destinato a consumatori né a minori, e la registrazione con indirizzi email personali o di provider gratuiti non è consentita. Non raccogliamo consapevolmente dati personali di minori come utenti del servizio.

12. Modifiche a questa informativa

Potremo aggiornare questa informativa, ad esempio quando introdurremo nuove funzionalità o completeremo gli impegni indicati sopra. Ogni versione riporta un identificativo e una data: pubblicheremo le nuove versioni su questa pagina, ciascuna con il proprio identificativo e la propria data. La versione accettata alla registrazione viene registrata insieme alla data e all'ora di accettazione. *Ultimo aggiornamento: versione privacy-2026-08-03.*