Accordo sul trattamento dei dati personali (DPA)

Versione 1.0, in vigore dal 22/11/2026

Il presente accordo ("DPA") stabilisce le condizioni alle quali MazzMedia SRL tratta dati personali nell'erogazione del servizio assisto. Contiene le clausole richieste dall'articolo 28, paragrafo 3, del Regolamento (UE) 2016/679 ("GDPR") per i trattamenti svolti per conto del Cliente, e disciplina inoltre i limitati trattamenti che MazzMedia SRL svolge come titolare autonomo.

Il DPA è concluso tra il Cliente, come identificato nell'ordine o nel contratto che richiama i Termini di servizio di assisto ("Cliente"), e MazzMedia SRL, con sede in Via Eritrea 21, 20157 Milano (MI), P.IVA IT06825720961, PEC mazzmedia@pec.it, in persona del legale rappresentante pro tempore ("MazzMedia"). Il DPA si intende sottoscritto con l'ordine o il contratto, alla data di quest'ultimo.

1. Definizioni e interpretazione

1.1 Titolare, responsabile, interessato, dato personale, trattamento e violazione dei dati personali hanno il significato attribuito loro dal GDPR.

1.2 Normativa sulla protezione dei dati: il GDPR, il D.lgs. 196/2003 (Codice in materia di protezione dei dati personali) come modificato dal D.lgs. 101/2018, i provvedimenti dell'Autorità garante e ogni altra norma applicabile al trattamento.

1.3 Servizio: la piattaforma assisto come descritta nei Termini di servizio e nell'ordine o nel contratto.

1.4 Utenti finali: i visitatori che interagiscono con gli assistenti del Cliente sui suoi siti e canali.

1.5 Cliente finale: il titolare per conto del quale il Cliente, quando agisce come responsabile, tratta dati personali tramite il Servizio (sezione 2.3).

1.6 Sub-responsabile: il fornitore di cui MazzMedia si avvale per svolgere specifiche attività di trattamento per conto del Cliente, elencato nell'Allegato C.

1.7 Autorità pubblica: qualsiasi autorità giudiziaria, amministrativa, di polizia o di controllo che abbia il potere di chiedere o imporre l'accesso a dati personali.

1.8 Clausole contrattuali tipo: le clausole adottate dalla Commissione europea con la decisione di esecuzione (UE) 2021/914 del 4 giugno 2021, e successive modifiche o sostituzioni.

1.9 Gli allegati sono parte integrante del DPA. I termini non definiti qui hanno il significato indicato nei Termini di servizio. Per quanto riguarda la protezione dei dati personali, in caso di contrasto tra il DPA e i Termini di servizio **prevale il DPA**; in caso di contrasto tra il DPA e un accordo sul trattamento dei dati sottoscritto separatamente tra le parti, prevale quest'ultimo.

2. Ruoli delle parti

2.1 MazzMedia come responsabile. Per i dati personali trattati tramite il Servizio per conto del Cliente, il Cliente è titolare e MazzMedia è responsabile del trattamento. L'oggetto, la natura, le finalità, la durata, i tipi di dati e le categorie di interessati sono descritti nell'Allegato A1.

2.2 MazzMedia come titolare autonomo. MazzMedia tratta come titolare autonomo, secondo la propria informativa privacy, i dati degli amministratori e degli utenti del Cliente che accedono alla piattaforma, e i dati di utilizzo del Servizio in forma aggregata o anonima, per gestire, proteggere e migliorare il Servizio, come descritto nell'Allegato A2. Tali dati non contengono il testo delle conversazioni né i dati di contatto degli Utenti finali, e non sono comunicati a terzi in forma che consenta di identificare il Cliente o un interessato. Ciascuna parte risponde in autonomia dei trattamenti di cui è titolare.

2.3 Cliente che agisce come responsabile. Se il Cliente utilizza il Servizio per conto di un Cliente finale, come nel caso di un'agenzia che gestisce l'assistente di un proprio cliente, **MazzMedia agisce come sub-responsabile del Cliente**. Il Cliente garantisce di aver ottenuto dal Cliente finale l'autorizzazione a ricorrere a MazzMedia e ai sub-responsabili dell'Allegato C, e che le istruzioni impartite a MazzMedia sono coerenti con l'accordo sul trattamento in essere con il Cliente finale. In tal caso gli obblighi del presente DPA si applicano in quanto compatibili, e il Cliente resta il solo interlocutore di MazzMedia.

3. Obblighi del Cliente

3.1 Il Cliente determina le finalità del trattamento e resta responsabile del rispetto della normativa sulla protezione dei dati, in particolare della base giuridica dei trattamenti, dell'informativa agli Utenti finali prevista dagli articoli 13 e 14 del GDPR, dell'avviso che stanno interagendo con un sistema di intelligenza artificiale e della raccolta dei consensi eventualmente necessari, anche per i cookie e gli strumenti di tracciamento che sceglie di attivare.

3.2 Il Cliente garantisce che i contenuti che carica e le istruzioni che impartisce sono leciti e non violano diritti di terzi.

3.3 Il Cliente non carica nella base di conoscenza, e non configura l'assistente per raccogliere, categorie particolari di dati personali o dati relativi a condanne penali e reati, salvo accordo scritto con MazzMedia.

4. Obblighi di MazzMedia

4.1 MazzMedia tratta i dati personali **soltanto su istruzione documentata del Cliente** e nella misura necessaria all'erogazione del Servizio. Costituiscono istruzioni documentate i Termini di servizio, il presente DPA e le configurazioni impostate dal Cliente nella piattaforma, come la base di conoscenza, il flusso dell'assistente, la raccolta dei lead e le integrazioni attivate. MazzMedia informa senza ritardo il Cliente se ritiene che un'istruzione violi la normativa sulla protezione dei dati.

4.2 MazzMedia non utilizza i dati personali trattati per conto del Cliente per finalità proprie, **né per addestrare modelli di intelligenza artificiale**.

4.3 MazzMedia esegue le istruzioni scritte del Cliente di rettificare, esportare o cancellare dati personali, o di interrompere un trattamento non autorizzato.

4.4 MazzMedia garantisce che il personale autorizzato a trattare i dati personali sia vincolato alla riservatezza, conosca gli obblighi derivanti dal presente DPA e dalla normativa sulla protezione dei dati, e acceda ai dati solo nella misura necessaria all'erogazione del Servizio, all'assistenza richiesta dal Cliente o alla risoluzione di problemi tecnici.

4.5 MazzMedia informa il Cliente dei cambiamenti normativi che possono ragionevolmente compromettere l'esecuzione del Servizio o del presente DPA.

5. Sicurezza

5.1 MazzMedia adotta misure tecniche e organizzative adeguate al rischio ai sensi dell'articolo 32 del GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'oggetto, del contesto e delle finalità del trattamento. Le misure in vigore sono descritte nell'Allegato B e comprendono, tra l'altro, la cifratura dei dati, la capacità di assicurare la riservatezza, l'integrità e la disponibilità dei sistemi, la capacità di ripristinare l'accesso ai dati in caso di incidente e una verifica periodica dell'efficacia delle misure.

5.2 MazzMedia può aggiornare le misure nel tempo, a condizione di non ridurre il livello complessivo di protezione.

6. Violazioni dei dati personali

6.1 MazzMedia notifica al Cliente, senza ingiustificato ritardo e comunque **entro 48 ore da quando ne è venuta a conoscenza**, qualsiasi violazione dei dati personali trattati per conto del Cliente.

6.2 La notifica contiene, nella misura in cui sono disponibili: la natura della violazione, le categorie e il numero approssimativo di interessati e di registrazioni coinvolti; le probabili conseguenze; le misure adottate o proposte da MazzMedia per porvi rimedio e attenuarne gli effetti; il nome e i dati di contatto di un referente. Le informazioni non disponibili subito sono fornite in fasi successive senza ulteriore ritardo.

6.3 Le notifiche all'autorità di controllo e le comunicazioni agli interessati spettano al Cliente, con la collaborazione di MazzMedia. Salvo obbligo di legge, MazzMedia non comunica la violazione a terzi senza il consenso scritto del Cliente.

7. Richieste delle autorità pubbliche

7.1 Se riceve da un'Autorità pubblica una richiesta vincolante di accesso ai dati personali trattati per conto del Cliente, MazzMedia **ne informa senza ritardo il Cliente**, con una sintesi della richiesta, salvo

che la legge lo vieti. Se la comunicazione è vietata, MazzMedia si adopera in modo ragionevole per ottenere che il divieto sia rimosso, così da fornire al Cliente quante più informazioni possibile.

7.2 MazzMedia valuta la legittimità di ogni richiesta, comunica solo i dati strettamente necessari a soddisfarla e può contestarla se ritiene, dopo un'attenta valutazione, che vi siano fondati motivi per considerarla illegittima.

8. Trasferimenti fuori dallo Spazio economico europeo

8.1 MazzMedia, o un sub-responsabile, trasferisce dati personali fuori dallo Spazio economico europeo soltanto in presenza di una delle garanzie previste dal Capo V del GDPR: una decisione di adeguatezza, inclusa la certificazione del destinatario al Data Privacy Framework UE-USA, oppure le Clausole contrattuali tipo, integrate dalle misure supplementari eventualmente necessarie. I trasferimenti in corso e le relative garanzie sono indicati nell'Allegato C.

8.2 Se il Cliente ha sede fuori dallo Spazio economico europeo, le parti concludono su richiesta le Clausole contrattuali tipo nel modulo applicabile.

9. Sub-responsabili

9.1 Il Cliente concede a MazzMedia un'**autorizzazione generale** a ricorrere ai sub-responsabili elencati nell'Allegato C.

9.2 MazzMedia comunica al Cliente, per via elettronica e **con almeno 30 giorni di preavviso**, l'aggiunta o la sostituzione di un sub-responsabile, indicando le informazioni necessarie per valutarla. Il Cliente può opporsi per motivi ragionevoli legati alla protezione dei dati entro lo stesso termine. In caso di opposizione le parti cercano in buona fede una soluzione; se non la trovano, **il Cliente può recedere dal contratto relativo al Servizio interessato senza penali**, con rimborso della parte di corrispettivo già pagata e relativa al periodo non goduto.

9.3 In caso di urgenza, come la sostituzione di un fornitore per motivi di sicurezza o di continuità del Servizio, il preavviso può essere ridotto e la comunicazione avviene appena possibile, fermo il diritto di opposizione del Cliente.

9.4 MazzMedia impone a ciascun sub-responsabile, con contratto scritto, obblighi in materia di protezione dei dati sostanzialmente equivalenti a quelli del presente DPA, **resta pienamente responsabile verso il Cliente** del loro adempimento e lo informa se un sub-responsabile non li rispetta.

10. Richieste degli interessati e reclami

10.1 MazzMedia assiste il Cliente, con misure tecniche e organizzative adeguate, nel dare seguito alle richieste di esercizio dei diritti previsti dagli articoli da 15 a 22 del GDPR. Il Cliente può consultare, esportare e cancellare conversazioni e lead dall'area di amministrazione; per le richieste che non può gestire in autonomia, MazzMedia fornisce assistenza **entro 10 giorni lavorativi dalla richiesta**.

10.2 MazzMedia informa per iscritto il Cliente **entro 5 giorni lavorativi** se riceve direttamente una richiesta di un interessato, un reclamo o una comunicazione di un'autorità relativi ai dati trattati per conto del Cliente, e non vi risponde nel merito salvo istruzione del Cliente o obbligo di legge.

10.3 MazzMedia assiste inoltre il Cliente, fornendo le informazioni di cui dispone, negli adempimenti previsti dagli articoli da 32 a 36 del GDPR, comprese la valutazione d'impatto e l'eventuale consultazione preventiva dell'autorità di controllo.

11. Registro dei trattamenti

11.1 MazzMedia tiene il registro delle attività di trattamento svolte per conto dei propri clienti previsto dall'articolo 30, paragrafo 2, del GDPR, con le categorie di trattamento, i sub-responsabili, i trasferimenti fuori dallo Spazio economico europeo con le relative garanzie e la descrizione delle misure di sicurezza, e ne fornisce al Cliente un estratto relativo ai trattamenti che lo riguardano, su richiesta.

12. Verifiche

12.1 MazzMedia mette a disposizione del Cliente le informazioni necessarie a dimostrare il rispetto dell'articolo 28 del GDPR, anzitutto tramite il presente DPA, i suoi allegati, l'estratto del registro e la documentazione dei sub-responsabili, e risponde per iscritto ai questionari ragionevoli del Cliente.

12.2 Se tali informazioni non sono sufficienti, o se lo richiede un'autorità di controllo, il Cliente può svolgere una verifica, direttamente o tramite un revisore indipendente, vincolato alla riservatezza e non concorrente di MazzMedia, alle seguenti condizioni: preavviso scritto di almeno 30 giorni; **non più di una volta ogni 12 mesi**, salvo in seguito a una violazione dei dati; perimetro, date e modalità concordati in anticipo; svolgimento da remoto o durante l'orario lavorativo, senza accesso ai dati di altri clienti e senza compromettere la sicurezza del Servizio. I costi della verifica sono a carico del Cliente.

13. Integrazioni attivate dal Cliente

13.1 Il Cliente può attivare integrazioni con servizi di terzi, come CRM e strumenti di gestione dei progetti (ad esempio HubSpot, Salesforce, ClickUp), canali di messaggistica (ad esempio WhatsApp tramite Meta) e strumenti di misurazione (ad esempio Google Analytics 4 e Meta Pixel). Quando un'integrazione è attiva, MazzMedia trasmette i dati al servizio indicato su istruzione del Cliente e tramite gli account del Cliente.

13.2 Tali servizi sono scelti dal Cliente e operano sulla base del rapporto contrattuale tra il Cliente e il relativo fornitore: **non sono sub-responsabili di MazzMedia** ai sensi della sezione 9. Il Cliente è responsabile di valutarne la conformità e di regolare con loro il trattamento dei dati.

14. Durata, restituzione e cancellazione

14.1 Il DPA ha la stessa durata del rapporto contrattuale relativo al Servizio. Le disposizioni che per loro natura devono sopravvivere alla cessazione, come quelle sulla riservatezza, sulla restituzione e sulla cancellazione dei dati, restano in vigore fino al loro completamento.

14.2 Durante il rapporto i dati sono conservati secondo i tempi indicati nell'Allegato A1, che MazzMedia applica con procedure automatiche di cancellazione. Il Cliente può cancellare in qualsiasi momento singole conversazioni e singoli lead dall'area di amministrazione.

14.3 Alla cessazione del rapporto, il Cliente può richiedere **entro 30 giorni l'esportazione dei lead e delle conversazioni** in un formato di uso comune. Decorso tale termine, MazzMedia cancella i dati personali trattati per conto del Cliente **entro i successivi 30 giorni**, salvo che la legge ne imponga la conservazione. Le copie presenti nei backup sono cancellate al termine del ciclo di rotazione dei backup, che **non supera 8 giorni**, e nel frattempo non sono utilizzate. Su richiesta, MazzMedia conferma per iscritto l'avvenuta cancellazione.

14.4 Se un cambiamento della normativa sulla protezione dei dati impedisce a una parte di adempiere in tutto o in parte ai propri obblighi, le parti possono concordare di sospendere il trattamento interessato fino al suo adeguamento. Se l'adeguamento non è possibile entro 30 giorni lavorativi, ciascuna parte può recedere dal contratto relativo al Servizio interessato con comunicazione scritta.

15. Responsabilità

15.1 La responsabilità delle parti per le violazioni del presente DPA è regolata dall'articolo 82 del GDPR e, nei limiti consentiti dalla legge, dalle limitazioni previste nei Termini di servizio o nel contratto.

16. Modifiche

16.1 MazzMedia può modificare il DPA per adeguarlo a cambiamenti normativi, a indicazioni delle autorità o all'evoluzione del Servizio, con preavviso di 30 giorni per via elettronica, purché le modifiche non riducano il livello di protezione dei dati. Ogni versione è registrata nell'Allegato D. L'aggiornamento dell'elenco dei sub-responsabili segue la procedura della sezione 9.

17. Legge applicabile e foro

17.1 Il DPA è regolato dalla **legge italiana**. Per ogni controversia relativa al DPA è competente il **foro di Milano**.

18. Contatti

18.1 Per le comunicazioni relative al DPA, alle richieste degli interessati e alle violazioni dei dati: privacy@mazzmedia.com e PEC mazzmedia@pec.it.

Allegato A1. Trattamenti svolti come responsabile

Elemento	Descrizione
Oggetto	Erogazione del Servizio per conto del Cliente: assistenti basati su intelligenza artificiale integrati nei siti e nei canali del Cliente, alimentati da una base di conoscenza fornita dal Cliente.
Natura e finalità	Gestione delle conversazioni tra gli Utenti finali e l'assistente; generazione delle risposte tramite modelli di intelligenza artificiale; trascrizione e sintesi vocale, se attivate; raccolta e gestione dei contatti (lead), se attivata; punteggio di priorità dei lead a supporto del Cliente; statistiche di utilizzo per il Cliente nell'area di amministrazione; notifiche agli amministratori del Cliente; invio dei dati alle integrazioni attivate dal Cliente.
Categorie di interessati	Utenti finali che interagiscono con l'assistente; persone che lasciano i propri dati di contatto tramite l'assistente; persone eventualmente menzionate nei contenuti caricati dal Cliente.
Tipi di dati	Testo dei messaggi scambiati con l'assistente e audio dei messaggi vocali, se la funzione è attiva; dati di contatto inseriti dall'Utente finale (nome, e-mail, telefono, azienda, ruolo, sito web, città, CAP), note di passaggio a un operatore, fonte del consenso e punteggio del lead; pagine del sito visitate durante la conversazione; dati tecnici di utilizzo (indirizzo IP, user agent, tipo di dispositivo, sistema operativo, browser, paese, identificativi della conversazione e della sessione); dati personali eventualmente presenti nei contenuti caricati dal Cliente.
Categorie particolari di dati	**Non previste.** L'assistente non è progettato per raccoglierle; se un Utente finale le inserisce spontaneamente in una conversazione, sono trattate come il resto della conversazione e cancellate con essa.
Durata e frequenza	Continuativa, per la durata del rapporto contrattuale, salvo i tempi di conservazione indicati sotto.
Conservazione	Conversazioni e relativi messaggi: **12 mesi dalla creazione della conversazione**, poi cancellazione automatica. Lead: **12 mesi dalla raccolta**, poi cancellazione automatica. Messaggi salvati nel browser dell'Utente finale: **12 mesi dall'ultimo salvataggio**. Audio dei messaggi vocali: **non conservato dopo la trascrizione**. Dati tecnici di utilizzo: **12 mesi dalla registrazione**, poi cancellazione automatica. Il Cliente può cancellare prima conversazioni e lead dall'area di amministrazione.
Sub-responsabili	Elencati nell'Allegato C.

Allegato A2. Trattamenti svolti come titolare autonomo

Elemento	Descrizione
Finalità	Gestione degli account di accesso alla piattaforma e del rapporto con il Cliente; sicurezza e prevenzione degli abusi; monitoraggio del funzionamento del Servizio; miglioramento del Servizio sulla base di dati aggregati o anonimi.

Elemento	Descrizione
Categorie di interessati	Amministratori e utenti del Cliente che accedono alla piattaforma.
Tipi di dati	Dati di account (nome, e-mail, ruolo, credenziali e passkey, preferenze di notifica) e registri di accesso. Statistiche aggregate di utilizzo e registro anonimo degli argomenti delle domande, che riporta solo la categoria dell'argomento, la data e l'assistente, senza testo dei messaggi né riferimenti alla conversazione o all'Utente finale.
Base giuridica	Esecuzione del contratto con il Cliente e legittimo interesse di MazzMedia alla sicurezza e al miglioramento del Servizio.
Conservazione	Dati di account: per la durata del rapporto e successivamente nei limiti previsti dall'informativa privacy di MazzMedia. Registro anonimo degli argomenti: 24 mesi.
Informativa	Informativa privacy di MazzMedia SRL: assisto.mazzmedia.com/privacy.

Allegato B. Misure tecniche e organizzative

Ambito	Misure
Controllo dell'accesso fisico	MazzMedia non gestisce data center propri. L'infrastruttura è fornita dai sub-responsabili dell'Allegato C, che applicano controlli di accesso fisico ai propri data center secondo standard riconosciuti, come SOC 2 o ISO 27001.
Controllo dell'accesso ai sistemi	Accesso alle console di infrastruttura limitato al personale autorizzato, con account nominativi presso i fornitori. Accesso all'area di amministrazione del Servizio con credenziali personali e supporto alle passkey; account creati solo su invito. Ambienti di anteprima protetti da autenticazione.
Controllo dell'accesso ai dati	Accesso secondo il principio del minimo privilegio. Ruoli distinti per i proprietari e per gli utenti assegnati a un singolo assistente. Il personale di MazzMedia accede ai dati del Cliente solo per assistenza o per risolvere problemi tecnici.
Cifratura	Comunicazioni cifrate in transito con TLS. Database e archivi cifrati a riposo presso i fornitori di infrastruttura. Testo dei messaggi delle conversazioni e dati di contatto dei lead (e-mail, nome, telefono, azienda, ruolo, sito, città, CAP, note) cifrati a livello applicativo con **AES-256-GCM**, con chiavi distinte per ciascun assistente, prima di essere salvati nel database.
Separazione dei dati	Dati di ciascun Cliente separati logicamente nel database tramite regole di accesso a livello di riga (row level security) e controlli applicativi sull'assistente e sul dominio di appartenenza.
Monitoraggio	Monitoraggio degli errori configurato senza invio dei dati personali predefiniti (indirizzi IP, cookie, intestazioni) e con registrazioni di sessione in cui testo, campi e contenuti multimediali sono mascherati.

Ambito	Misure
Disponibilità e ripristino	Infrastruttura gestita da fornitori cloud con ridondanza; backup automatici del database gestiti dal fornitore del database, conservati per 8 giorni; monitoraggio degli errori dell'applicazione.
Conservazione e minimizzazione	Cancellazione automatica giornaliera di conversazioni, lead e dati tecnici di utilizzo oltre i tempi dell'Allegato A1. Audio dei messaggi vocali non conservato. Statistiche sugli argomenti tenute in forma anonima, senza testo dei messaggi.
Sviluppo e gestione delle modifiche	Codice sotto controllo di versione; rilasci in produzione tracciati e reversibili; ambienti di anteprima protetti per le modifiche in sviluppo; chiavi e segreti conservati come variabili d'ambiente e non nel codice.
Organizzazione	Personale autorizzato vincolato alla riservatezza; procedura di gestione e notifica delle violazioni dei dati; revisione periodica delle misure.

Allegato C. Sub-responsabili

Elenco aggiornato al 22/11/2026. Le modifiche sono comunicate secondo la sezione 9.

Sub-responsabile	Attività	Luogo del trattamento	Garanzie per il trasferimento
OpenAI Ireland Ltd, con OpenAI OpCo LLC	Modelli di intelligenza artificiale per le risposte, gli embedding della base di conoscenza, il punteggio dei lead, la trascrizione e la sintesi vocale.	Unione europea e Stati Uniti	Clausole contrattuali tipo e Data Privacy Framework UE-USA
Supabase Inc.	Database, autenticazione degli amministratori, archiviazione dei dati del Servizio.	Unione europea (Germania, Francoforte)	Clausole contrattuali tipo
Vercel Inc.	Hosting dell'applicazione ed esecuzione delle funzioni, archiviazione dei file caricati (PDF), statistiche di traffico e prestazioni senza cookie.	Unione europea (Germania, Francoforte) per le funzioni; rete di distribuzione globale per i contenuti statici	Clausole contrattuali tipo e Data Privacy Framework UE-USA
Functional Software Inc. (Sentry)	Monitoraggio degli errori dell'applicazione.	Unione europea (Germania)	Clausole contrattuali tipo
MailUp S.p.A.	Invio delle e-mail di servizio e di notifica agli amministratori del Cliente, che possono contenere dati dei lead.	Unione europea (Italia)	Non applicabile: trattamento nell'Unione europea

Allegato D. Storico delle versioni

Versione	Data	Modifiche
1.0	22/11/2026	Prima versione.

Sottoscrizione

Le parti sottoscrivono il presente DPA, versione 1.0, comprensivo degli allegati A1, A2, B, C e D.

Il Cliente

Ragione sociale

Nome e qualifica del firmatario

Luogo e data

Firma

MazzMedia SRL

Nome e qualifica del firmatario

Luogo e data

Firma