

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

(Data Processing Agreement — art. 28 Reg. UE 2016/679 «GDPR»)

Tra le Parti

Webgas S.r.l., P.IVA 04564820613, con sede legale in Via Vittime di Nassiriya 1, 82100 Benevento (BN), fornitore della piattaforma **Uptonica** (di seguito il «**Responsabile**» o «Uptonica»);

e

il **Cliente**, come identificato nell'account / order form con cui accetta i Termini di Servizio di Uptonica (di seguito il «**Titolare**»);

congiuntamente le «Parti».

Il presente Accordo («DPA») costituisce **parte integrante dei Termini di Servizio** di Uptonica ed è **accettato per via elettronica** dal Titolare con l'accettazione dei Termini / la sottoscrizione dell'order form, ai sensi dell'**art. 28(9) GDPR** («in forma scritta, anche elettronica»; non è richiesta firma autografa). Disciplina il trattamento dei dati personali effettuato dal Responsabile per conto del Titolare; in caso di conflitto sulle materie di protezione dei dati, prevale il presente DPA.

Art. 1 — Definizioni

I termini «dato personale», «trattamento», «titolare del trattamento», «responsabile del trattamento», «interessato», «violazione dei dati personali», «autorità di controllo» hanno il significato di cui all'art. 4 GDPR. «Diritto applicabile in materia di protezione dei dati» indica il GDPR e la normativa italiana di adeguamento (D.lgs. 196/2003 come modificato). «Sub-responsabile» indica qualsiasi terzo incaricato dal Responsabile di trattare dati personali per conto del Titolare. «SCC» indica le Clausole Contrattuali Standard di cui alla Decisione di esecuzione (UE) 2021/914.

Art. 2 — Oggetto, durata, natura e finalità

2.1 Il Responsabile tratta i dati personali esclusivamente per erogare i servizi della piattaforma Uptonica (assistente conversazionale multicanale, CRM e gestione contatti, arricchimento del catalogo tramite AI, automazioni, integrazione email-to-CRM, fatturazione), per conto e su istruzione del Titolare.

2.2 Natura, finalità del trattamento, categorie di dati personali e di interessati sono descritte nell'**Allegato I**.

2.3 Il DPA ha efficacia per tutta la durata del Contratto e fino al completamento delle operazioni di restituzione o cancellazione dei dati di cui all'art. 10.

Art. 3 — Istruzioni documentate

3.1 Il Responsabile tratta i dati personali soltanto su **istruzioni documentate** del Titolare — comprese quelle relative ai trasferimenti verso paesi terzi — salvo che lo imponga il diritto dell'Unione o nazionale, nel qual caso ne informa il Titolare prima del trattamento (salvo divieto di legge). Il Contratto, il presente DPA e l'uso configurato della piattaforma costituiscono le istruzioni iniziali complete del Titolare.

3.2 Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il Diritto applicabile in materia di protezione dei dati.

Art. 4 — Riservatezza

Il Responsabile garantisce che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, e che l'accesso ai dati personali sia limitato al personale che deve trattarli per l'esecuzione del Contratto.

Art. 5 — Misure di sicurezza (art. 32)

Il Responsabile adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, descritte nell'**Allegato II**, tenuto conto dello stato dell'arte, dei costi e della natura, oggetto, contesto e finalità del trattamento. Il Responsabile può aggiornare tali misure purché non ne riduca il livello di sicurezza.

Art. 6 — Sub-responsabili

6.1 Il Titolare conferisce al Responsabile un'**autorizzazione generale** al ricorso a sub-responsabili. L'elenco dei sub-responsabili in essere è nell'**Allegato III** ed è mantenuto aggiornato su pagina pubblica versionata.

6.2 Il Responsabile informa il Titolare di ogni aggiunta o sostituzione di un sub-responsabile con un **preavviso di almeno 30 giorni**, dando al Titolare la possibilità di opporsi per motivi ragionevoli connessi alla protezione dei dati. In caso di opposizione non risolvibile, il Titolare può recedere dalla parte di servizio interessata.

6.3 Il Responsabile impone a ciascun sub-responsabile, mediante contratto, gli **stessi obblighi** di protezione dei dati previsti dal presente DPA (art. 28(4) GDPR), e **risponde pienamente** nei confronti del Titolare dell'operato dei propri sub-responsabili.

Art. 7 — Assistenza al Titolare

7.1 Tenuto conto della natura del trattamento, il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate, nella misura del possibile, per dar seguito alle richieste di esercizio dei diritti degli interessati (artt. 12-23 GDPR). La piattaforma mette a disposizione funzioni di **cancellazione (art. 17)** e **portabilità/esportazione (art. 20)** per singolo interessato.

7.2 Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR (sicurezza, notifica delle violazioni, valutazione d'impatto e consultazione preventiva), tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile.

Art. 8 — Violazioni dei dati personali

Il Responsabile notifica al Titolare ogni violazione dei dati personali **senza ingiustificato ritardo e comunque entro 72 ore** dal momento in cui ne viene a conoscenza, fornendo le informazioni di cui all'art. 33(3) GDPR ragionevolmente disponibili, per consentire al Titolare di adempiere ai propri obblighi di notifica all'autorità e agli interessati.

Art. 9 — Trasferimenti internazionali

9.1 Il trattamento avviene prevalentemente all'interno dello SEE (hosting in Germania). Per i sub-responsabili stabiliti fuori dallo SEE (indicati nell'Allegato III), il trasferimento è legittimato mediante le **Clausole Contrattuali Standard (SCC) — Decisione (UE) 2021/914, Modulo 2 (titolare→responsabile)**, che si intendono **incorporate per riferimento** e integrate dalle scelte di cui all'Allegato III; ove il Responsabile agisca verso il sub-responsabile, si applica il Modulo 3.

9.2 Il Responsabile adotta le **misure supplementari** specifiche descritte nell'Allegato II (in particolare cifratura in transito e at-rest, minimizzazione, controllo accessi) a integrazione delle SCC, ai sensi della giurisprudenza «Schrems II».

9.3 Le scelte richieste dalle SCC sono così determinate: Clausola 7 (docking) — **applicabile**; Clausola 9 — autorizzazione **generale**, preavviso 30 giorni; Clausola 11 — meccanismo di reclamo dell'interessato **non** opzionale-indipendente salvo diverso accordo; Clausola 17 — legge **italiana**; Clausola 18 — foro di **Benevento**.

Art. 10 — Cancellazione o restituzione

10.1 Alla cessazione del Contratto, a scelta del Titolare, il Responsabile **cancella** o **restituisce** tutti i dati personali e cancella le copie esistenti, salvo obblighi di conservazione previsti dal diritto dell'Unione o nazionale (es. obblighi fiscali/contabili sui documenti d'ordine e sulle firme elettroniche).

10.2 **Retention.** Per impostazione predefinita i dati sono conservati per la durata del rapporto; il Titolare può concordare con il Responsabile finestre di conservazione e cancellazione per il proprio spazio (Allegato IV).

Art. 11 — Audit

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consente e contribuisce ad **audit**, comprese le ispezioni, condotti dal Titolare o da un revisore da esso incaricato, con **preavviso ragionevole (almeno 30 giorni)**, non più di una volta l'anno salvo richiesta motivata di un'autorità o a seguito di una violazione, nel rispetto della riservatezza e della sicurezza degli altri clienti del Responsabile (ambiente multi-tenant).

Art. 12 — Responsabilità e durata

La responsabilità delle Parti è disciplinata dal Contratto principale e dal GDPR. Il presente DPA decorre dalla sottoscrizione del Contratto e cessa con esso, fatte salve le clausole destinate a sopravvivere (riservatezza, cancellazione, audit relativi al periodo).

Art. 13 — Legge applicabile e foro

Il presente DPA è regolato dalla **legge italiana**. Per ogni controversia è competente il foro di **Benevento**. Per i trasferimenti soggetti alle SCC restano ferme le previsioni inderogabili delle stesse.

Allegato I — Dettagli del trattamento

Voce	Contenuto
Categorie di interessati	Clienti finali e contatti/lead del Titolare; personale/utenti del Titolare.
Categorie di dati personali	Dati identificativi (nome, email, telefono); indirizzo; preferenze e consensi marketing; identificativi di canale (WhatsApp/Telegram/Meta); dati comportamentali e di attribuzione (UTM, gclid/fbclid, landing); contenuto delle conversazioni (testo, metadati AI, sentiment); dati d'ordine (i dati di pagamento sono tokenizzati e non conservati dal Responsabile); credenziali utente (password in hash, 2FA); firme elettroniche (dati del firmatario, IP, timestamp, hash).
Dati particolari (art. 9) / minori	Non raccolti strutturalmente. Il Titolare si impegna a non immettere dati particolari nei campi liberi salvo idonea base giuridica; trattamento di dati di minori escluso salvo istruzione e base giuridica del Titolare.
Natura e finalità	Hosting, elaborazione conversazioni, gestione contatti/CRM, arricchimento catalogo, automazioni, email-to-CRM, fatturazione — su istruzione del Titolare.
Durata	Durata del Contratto + periodo di restituzione/cancellazione.

Allegato II — Misure tecniche e organizzative (art. 32)

- **Cifratura in transito:** TLS/HTTPS su tutti gli endpoint; comunicazioni interne su rete privata.
- **Cifratura at-rest:** volume dati del database su **LUKS2** (AES-XTS); backup locali sul volume cifrato e backup fuori sede cifrati; cifratura applicativa delle credenziali/segrete e delle chiavi fornite dal cliente; chiave applicativa AES-256-GCM.
- **Controllo accessi:** autenticazione con token, RBAC (ruoli/permessi), autenticazione a due fattori; gestione segreti centralizzata e cifrata.
- **Isolamento:** architettura multi-tenant con scoping per tenant a livello applicativo e separazione per schema.
- **Tracciabilità:** registri di attività e registri di audit immutabili (append-only) per operazioni sensibili.
- **Continuità:** backup giornalieri cifrati con rotazione locale (7 gg) e off-site (30 gg); **RPO ≤ 24 ore** (cadenza giornaliera), **RTO obiettivo ≤ 8 ore**; ripristino verificato periodicamente.
- **Ubicazione:** infrastruttura nello SEE (Hetzner, Germania).

Allegato III — Sub-responsabili autorizzati

SEE = nessun SCC. Extra-SEE = SCC Modulo 2 (Dec. UE 2021/914) + misure supplementari (Allegato II). Categorie di dati/finalità per ciascuno disponibili su richiesta e sulla pagina pubblica versionata.

A. Sempre attivi

Area	Sub-responsabili UE (SEE)	Sub-responsabili extra-SEE (SCC)
Infrastruttura	Hetzner (DE)	—
Email	AWS SES (IE)	—
AI / LLM	—	Google (Gemini) (USA)
Ricerca / supporto	—	Serper, Tavily, ClickUp (USA)
Osservabilità / infra	Sentry (DE)	GitHub (USA); Cloudflare (multi-region UE/USA — SCC ove il traffico sia instradato fuori SEE)

B. Attivi solo se il Titolare attiva la funzione o l'integrazione corrispondente

Funzione	Sub-responsabili UE (SEE)	Sub-responsabili extra-SEE (SCC)
Canali di messaggistica	—	Postmark, Resend, Twilio, Meta (WhatsApp/IG/Messenger), Gmail API (USA); Telegram (senza Clausole Contrattuali Standard: da attivare solo previa valutazione del Titolare)
Assistente Lia (area riservata)	—	Anthropic, Cohere (USA)
Assistente in chat sul sito	Alibaba Cloud DashScope (DE), solo modelli premium scelti dal Titolare	Groq, OpenAI, Cohere, Helicone (USA); Anthropic, solo modelli premium scelti dal Titolare
Voce / telefonia	—	ElevenLabs, Telnyx (USA)
Contenuti / riunioni	—	fal.ai (USA); Vexa (trascrizione riunioni)
Pagamenti / fatturazione	Fattura24 (IT)	Stripe (USA)
E-commerce / ERP	Mexal (IT), WooCommerce (host UE)	Shopify, Salesforce Commerce Cloud (USA)
Analytics / Ads	Criteo (FR)	Google (Ads/GA4/Search Console/Merchant Center/GTM/Calendar), Klaviyo, Microsoft Advertising (USA); TikTok

Non ancora attivi (da aggiungere all'attivazione, con preavviso): Pinterest.

Allegato IV — Conservazione (retention)

- **Default:** conservazione per la durata del rapporto (nessuna cancellazione automatica).
- **Su istruzione del Titolare:** il Responsabile applica le finestre di conservazione e cancellazione concordate per lo spazio del Titolare (es. consensi, contatti inattivi, conversazioni, log).

- Conservati per obbligo di legge anche oltre la cessazione: documenti d'ordine (obblighi fiscali), firme elettroniche (eIDAS / CAD), registri di audit.
- **Diritto all'oblio (art. 17):** cancellazione/anonimizzazione per singolo interessato già disponibile.

Accettazione

Il presente DPA è parte dei Termini di Servizio di Uptonica ed è **accettato per via elettronica** dal Titolare con l'accettazione dei Termini / la sottoscrizione dell'order form (art. 28(9) GDPR — forma scritta elettronica; click-accept / incorporazione per riferimento). La data e la versione accettata sono registrate. Il documento è disponibile in **formato durevole scaricabile (PDF)** e nella sua versione corrente sulla pagina pubblica </legal/dpa>, con l'elenco dei sub-responsabili su </legal/sub-processors> (preavviso 30 giorni delle modifiche).

Per i clienti **enterprise** che ne necessitino, è disponibile su richiesta una **copia firmata separatamente** del presente DPA (annex sottoscrivibile), senza che ciò sia condizione di validità.