DOCUMENTO IMMUTABILE · V1.0 · PUBBLICATO IL 30 APRILE 2026

Data Processing Addendum (Allegato A)

URL canonico: headformula.com/legal/dpa/v1.0

Il presente Data Processing Addendum (di seguito, il "**DPA**" o l'"**Allegato A**") costituisce parte integrante delle Condizioni Generali di Servizio Headformula sottoscritte dalle Parti e disciplina il trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del Regolamento UE 2016/679 (di seguito, il "**GDPR**"). In caso di conflitto tra il DPA e le Condizioni Generali in materia di protezione dei dati personali, prevarranno le previsioni del DPA.

Il Cliente agisce in qualità di Titolare del Trattamento (di seguito, il "**Titolare**") e nomina **Headformula S.r.l.**, con sede in Milano, P.IVA 14573160968, quale Responsabile del Trattamento (di seguito, il "**Responsabile**") per le attività di trattamento di dati personali svolte nell'ambito dei servizi previsti dai Preventivi accettati.

1. Oggetto, natura e finalità del trattamento

Il Responsabile tratta dati personali per conto del Titolare al solo fine di eseguire i servizi descritti nei Preventivi accettati, includendo a titolo esemplificativo: gestione di campagne di advertising digitale, attività di email marketing e CRM, analisi di dati di campagne e di sito web, sviluppo e manutenzione di siti web ed e-commerce, gestione di canali social, retargeting e attività di profilazione su istruzioni del Titolare. Il trattamento è limitato a quanto strettamente necessario all'esecuzione dei servizi e si svolge sulla base delle istruzioni documentate del Titolare, comprese le presenti Condizioni e i Preventivi.

Sono escluse dal presente DPA, e oggetto di trattamento autonomo da parte di Headformula in qualità di **Titolare separato**, le attività di trattamento svolte da Headformula per finalità proprie, quali tra l'altro: fatturazione e adempimenti contabili, gestione del proprio personale e collaboratori, archivi commerciali interni, attività di marketing diretto verso il Cliente, log tecnici e operativi del proprio personale di sviluppo, gestione del rapporto contrattuale con il Cliente. Per tali trattamenti, Headformula osserva autonomamente gli obblighi previsti dal GDPR e fornisce idonea informativa ai propri interessati.

2. Categorie di dati e di interessati

I dati oggetto di trattamento includono: dati anagrafici (nome, cognome), dati di contatto (email, telefono, indirizzo), dati fiscali e di pagamento ove pertinenti, dati di navigazione e identificativi tecnici (cookie, log, indirizzo IP, identificatori device), dati comportamentali e di interazione con campagne e contenuti digitali, dati derivanti da profilazione effettuata sulle piattaforme advertising su istruzione del Titolare.

Le categorie di interessati comprendono: clienti e prospect del Titolare, utenti dei suoi siti web e canali digitali, iscritti a newsletter, lead acquisiti tramite campagne marketing, dipendenti e collaboratori del Titolare ove rilevanti per l'esecuzione dei servizi.

Il Responsabile non tratta categorie particolari di dati ex art. 9 GDPR salvo specifica istruzione scritta del Titolare.

3. Durata del trattamento

Il trattamento ha durata pari a quella del rapporto contrattuale con il Titolare e cessa al termine dell'ultimo Preventivo eseguito o alla revoca delle Condizioni, salvo il tempo strettamente necessario alla restituzione o cancellazione dei dati di cui all'art. 11 del presente DPA.

4. Obblighi del Responsabile

Il Responsabile si impegna a:

a. trattare i dati personali esclusivamente sulla base delle istruzioni documentate del Titolare, salvo quando ciò sia richiesto dal diritto dell'Unione o dello Stato membro applicabile; in tal caso, il Responsabile informa il Titolare prima del trattamento, salvo divieti normativi;
b. garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adottare tutte le misure di sicurezza richieste dall'art. 32 GDPR, come dettagliate all'art. 5 del presente DPA;
d. assistere il Titolare nell'adempimento degli obblighi di cui agli artt. 32-36 GDPR (sicurezza, notifica di violazioni, valutazioni d'impatto, consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;
e. assistere il Titolare nel dare seguito alle richieste degli interessati per l'esercizio dei loro diritti ex artt. 12-22 GDPR, mediante misure tecniche e organizzative adeguate;
f. mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR.

5. Misure tecniche e organizzative di sicurezza

Il Responsabile attua misure tecniche e organizzative adeguate ex art. 32 GDPR, incluse: cifratura dei dati in transito (TLS 1.2+) e a riposo ove tecnicamente possibile; controllo degli accessi basato sul principio del minimo privilegio, con autenticazione a più fattori per i sistemi che ospitano dati personali; segregazione logica degli ambienti di sviluppo, staging e produzione; backup periodici e procedure di disaster recovery; logging degli accessi e delle operazioni rilevanti su dati personali; aggiornamento regolare di software e sistemi; formazione periodica del personale autorizzato. Le misure di sicurezza sono soggette a revisione periodica e possono essere aggiornate per riflettere lo stato dell'arte e l'evoluzione del rischio, fermo restando il livello di protezione complessivo.

6. Sub-Responsabili

Il Titolare autorizza in via generale il Responsabile a ricorrere a Sub-Responsabili per delegare specifiche attività di trattamento. Il Responsabile si impegna a:

a. selezionare Sub-Responsabili che offrano garanzie sufficienti in termini di misure tecniche e organizzative adeguate ex art. 28(4) GDPR;
b. imporre ai Sub-Responsabili, mediante contratto scritto, gli stessi obblighi di protezione dei dati previsti dal

presente DPA;
c. mantenere e fornire al Titolare, su richiesta, l'elenco aggiornato dei Sub-Responsabili attivi.

In caso di nuova nomina o sostituzione di un Sub-Responsabile, il Responsabile informa il Titolare con preavviso di almeno **14 giorni** mediante email, durante i quali il Titolare può opporsi motivatamente per ragioni connesse alla protezione dei dati. In caso di opposizione motivata, le Parti si impegnano in buona fede a trovare una soluzione alternativa; in mancanza di accordo entro 30 giorni, ciascuna Parte può recedere senza penalità dai Preventivi che richiedevano l'utilizzo di tale Sub-Responsabile. Il Responsabile risponde dell'operato dei Sub-Responsabili nei confronti del Titolare come del proprio.

7. Trasferimenti di dati al di fuori dello Spazio Economico Europeo

Il Titolare prende atto che il Responsabile, nell'esecuzione dei servizi, potrebbe effettuare o consentire trasferimenti di dati personali verso Paesi al di fuori dello Spazio Economico Europeo (di seguito, "**Paesi Terzi**") nei seguenti casi tipici:

a. utilizzo di strumenti, piattaforme o servizi cloud forniti da provider con sede o infrastrutture in Paesi Terzi (a titolo esemplificativo: piattaforme di advertising digitale globali, strumenti di analytics, servizi di intelligenza artificiale, soluzioni di hosting o storage);
b. ricorso a Sub-Responsabili con sede in Paesi Terzi nel rispetto dell'art. 6 del presente DPA;
c. accesso remoto occasionale ai sistemi da parte di personale autorizzato del Responsabile durante trasferte di lavoro all'estero, limitato al tempo strettamente necessario.

Per i trasferimenti verso Paesi Terzi privi di decisione di adeguatezza della Commissione Europea, il Responsabile garantisce l'adozione di garanzie appropriate ex art. 46 GDPR, in via prioritaria mediante le **Clausole Contrattuali Standard (SCCs)** approvate dalla Commissione Europea con Decisione di esecuzione UE 2021/914 del 4 giugno 2021, integrate, ove necessario, da misure supplementari di natura tecnica, organizzativa o contrattuale per garantire un livello di protezione sostanzialmente equivalente a quello previsto nello Spazio Economico Europeo.

Il Responsabile effettua, nei casi richiesti, una valutazione dell'impatto del trasferimento (Transfer Impact Assessment) ai sensi delle raccomandazioni dell'European Data Protection Board e si impegna a fornire al Titolare, su richiesta, la documentazione comprovante l'adozione delle garanzie applicabili.

8. Violazione di dati personali (data breach)

In caso di violazione di dati personali di cui il Responsabile venga a conoscenza, il Responsabile informa il Titolare senza ingiustificato ritardo e comunque **entro 48 ore** dalla constatazione della violazione, fornendo tutte le informazioni utili affinché il Titolare possa adempiere agli obblighi di notifica al Garante e di comunicazione agli interessati ex artt. 33-34 GDPR. La comunicazione al Titolare include: descrizione della natura della violazione, categorie e numero approssimativo di interessati e di record coinvolti, conseguenze probabili, misure adottate o proposte per attenuare i possibili effetti negativi.

9. Diritti degli interessati e richieste delle autorità

Il Responsabile assiste il Titolare, mediante misure tecniche e organizzative adeguate, nel dar seguito alle richieste degli interessati relative all'esercizio dei diritti previsti dagli artt. 12-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione). Il Responsabile inoltra al Titolare senza ritardo ogni richiesta ricevuta direttamente dagli interessati o dalle autorità di controllo riguardante dati trattati per conto del Titolare, salvo divieti normativi.

10. Audit e ispezioni

Il Responsabile mette a disposizione del Titolare, su richiesta scritta motivata, tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dall'art. 28 GDPR. Il Titolare ha diritto di effettuare, anche tramite un revisore indipendente vincolato a obblighi di riservatezza, attività di audit con preavviso scritto di almeno 30 giorni e con cadenza non superiore a una volta all'anno, salvo casi documentati di sospetta violazione. L'audit si svolge negli orari lavorativi del Responsabile, con il minimo impatto sull'operatività e con costi a carico del Titolare richiedente, salvo che l'audit accerti inadempimenti significativi del Responsabile.

11. Cessazione del trattamento e restituzione dei dati

Alla cessazione del rapporto contrattuale, per qualsiasi causa, il Responsabile, a scelta del Titolare comunicata per iscritto, restituisce al Titolare o cancella tutti i dati personali trattati per conto dello stesso, comprese le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro richieda la conservazione dei dati. In assenza di scelta del Titolare entro 30 giorni dalla cessazione, il Responsabile procede alla cancellazione. Il Responsabile fornisce, su richiesta, conferma scritta dell'avvenuta cancellazione o restituzione.

12. Limitazione di responsabilità e disposizioni finali

Le previsioni del presente DPA si interpretano in coerenza con le Condizioni Generali di Servizio Headformula sottoscritte dalle Parti. Il presente DPA è regolato dalla legge italiana; per ogni controversia è competente in via esclusiva il Foro di Milano. Le clausole di limitazione di responsabilità previste dalle Condizioni Generali si applicano altresì agli inadempimenti del presente DPA, salvo che si tratti di violazioni del GDPR per le quali la legge non ammette limitazioni.

Sottoscrizione del DPA

L'accettazione del presente DPA avviene mediante sottoscrizione del Preventivo da parte del Cliente, che contiene la nomina espressa di Headformula S.r.l. quale Responsabile del Trattamento ex art. 28 GDPR ai termini del presente Allegato A.

---

headformula 45.4450°N / 9.1507°E

Headformula S.r.l. · Sede legale Milano · P.IVA 14573160968
DPA v1.0 — pubblicata il 30 aprile 2026 · canonical: headformula.com/legal/dpa/v1.0