ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI (DPA)

Nomina a Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR) — versione 2 — in vigore dal 9 novembre 2026

TRA il cliente che usa il servizio OglutForm, come identificato nel proprio account (di seguito il "**Titolare**"),

E Oglut S.r.l., con sede legale in Viale Tito Livio 67, 00136 Roma (RM), Italia, codice fiscale, partita IVA e numero di iscrizione al Registro delle imprese di Roma 15766701005, REA RM-1612571, capitale sociale 10.000 euro interamente versato, PEC oglut@legalmail.it, in persona del legale rappresentante pro tempore (di seguito il "**Responsabile**"),

di seguito, insieme, le "Parti".

1. Sottoscrizione e rapporto con le Condizioni generali

Il presente Accordo è accettato in modalità telematica dal Titolare quando crea il suo primo form o quando diventa proprietario di un form; da quel momento fa parte del contratto di servizio. L'accettazione è registrata nei sistemi del Responsabile con data e ora, versione e lingua dell'Accordo, impronta del documento, indirizzo IP, browser e account, e si conserva come prova per la durata del contratto e per i 10 anni successivi (termine ordinario di prescrizione, art. 2946 c.c.). L'Accordo fa parte delle Condizioni generali di servizio OglutForm (le "**Condizioni**"): per il trattamento dei dati dei contatti, se c'è un contrasto, prevale l'Accordo. Le parole con l'iniziale maiuscola non definite qui hanno il significato delle Condizioni. L'Accordo è disponibile in italiano e in inglese; in caso di differenze tra le due versioni vale l'art. 4.5 delle Condizioni.

2. Oggetto, natura e finalità del trattamento

Il Responsabile tratta i dati personali per conto del Titolare al solo fine di fornire il servizio OglutForm, cioè:

- ricevere e conservare i contatti inviati dalle persone che compilano i form del Titolare (form del sito del Titolare collegati al servizio, form creati con l'editor e inseriti nel sito, pagine dei form ospitate dal Responsabile);
- renderli consultabili, esportabili ed eliminabili dal Titolare e dai collaboratori che il Titolare invita, con il ruolo che il Titolare assegna;
- inviare, se il Titolare le attiva, le email di notifica al Titolare e le email di conferma a chi compila, e le risposte che il Titolare scrive dalla dashboard;
- proteggere i form dagli invii automatici e dagli abusi e garantire la sicurezza e il funzionamento del servizio.

Il Responsabile non tratta i dati dei contatti per finalità proprie: non li vende e non li usa per pubblicità, per profilazione o per addestrare sistemi di intelligenza artificiale.

3. Durata

L'Accordo ha la stessa durata del contratto di servizio. Gli obblighi di protezione dei dati restano fino alla cancellazione o alla restituzione dei dati (art. 12).

4. Interessati e tipi di dati

- **Interessati:** le persone che compilano i form del Titolare (per esempio visitatori, potenziali clienti, clienti, iscritti); i destinatari delle email inviate tramite il servizio; i collaboratori del Titolare, per i dati che li riguardano nei form del Titolare (ruolo, note e risposte che scrivono, azioni svolte).
- **Dati dei contatti:** i dati che il Titolare sceglie di raccogliere con i propri form (per esempio nome, email, telefono, messaggi, risposte), con i dati tecnici dell'invio: data e ora, indirizzo IP, browser (user agent), pagina di provenienza, lingua; lo stato e le note che il Titolare aggiunge; le email inviate e ricevute tramite il servizio in relazione a un contatto, con gli allegati.
- **Dati per la sicurezza:** registro tecnico delle richieste e impronte cifrate di indirizzi IP, destinatari e account usate per i limiti anti-abuso delle email (art. 11).
- **Categorie particolari di dati** (art. 9 GDPR) **e dati giudiziari** (art. 10): il servizio non offre misure specifiche per questi dati (per esempio la cifratura dei singoli campi). Il Titolare può raccogliere categorie particolari di dati solo sotto la propria responsabilità, se ha una base giuridica (art. 9 par. 2 GDPR), se ha valutato adeguate le misure dell'Allegato B e, quando serve, dopo una valutazione d'impatto (art. 35 GDPR). Non può raccogliere dati relativi a condanne penali e reati, salvo che una norma lo autorizzi (art. 10 GDPR). Il servizio non si usa per chiedere password, codici di sicurezza o dati di carte di pagamento (art. 10.1 delle Condizioni).

5. Istruzioni del Titolare

Il Responsabile tratta i dati solo secondo le istruzioni documentate del Titolare: il presente Accordo, le Condizioni e le impostazioni che il Titolare sceglie nel servizio (campi dei form, notifiche, email di conferma, collaboratori, eliminazioni, esportazioni), anche per i trasferimenti fuori dallo Spazio economico europeo (art. 13). Se il diritto dell'Unione europea o italiano gli impone un trattamento diverso, il Responsabile informa prima il Titolare, salvo che la legge lo vieti. Se un'istruzione gli sembra in contrasto con il GDPR o con altre norme sulla protezione dei dati, il Responsabile ne informa subito il Titolare.

6. Riservatezza

Possono accedere ai dati solo le persone autorizzate dal Responsabile che ne hanno bisogno per fornire il servizio, per l'assistenza richiesta dal Titolare o per la sicurezza, vincolate alla riservatezza. Gli accessi del personale all'account del Titolare con le credenziali di assistenza sono registrati come accessi del personale del Responsabile, con data, ora e azioni svolte, e il registro si conserva 12 mesi (art. 3.3 delle Condizioni).

7. Sicurezza

Il Responsabile adotta le misure tecniche e organizzative dell'Allegato B, adeguate al rischio (art. 32 GDPR), e le aggiorna nel tempo senza ridurne il livello di protezione.

8. Sub-responsabili

Il Titolare autorizza in modo generale il ricorso ai sub-responsabili dell'Allegato A. Il Responsabile impone loro, per contratto, obblighi di protezione dei dati non inferiori a quelli del presente

Accordo e risponde del loro operato verso il Titolare. Il Responsabile informa il Titolare, per email all'indirizzo dell'account, di ogni aggiunta o sostituzione di un sub-responsabile con almeno 15 giorni di preavviso; entro lo stesso termine il Titolare può opporsi per motivi ragionevoli legati alla protezione dei dati e, se le Parti non trovano una soluzione, far cessare il contratto senza costi, con il rimborso della parte non usata del periodo pagato e del credito che viene da pagamenti.

9. Diritti degli interessati e assistenza al Titolare

Il Titolare può cercare, esportare (CSV) ed eliminare i contatti direttamente dalla dashboard, anche per rispondere alle richieste degli interessati (accesso, cancellazione, portabilità, opposizione); per la rettifica dei dati di un contatto, che dalla dashboard non si possono modificare, e per i dati che la dashboard non esporta, il Responsabile interviene su richiesta del Titolare, senza costi. Se una richiesta arriva al Responsabile, il Responsabile la inoltra al Titolare senza rispondere nel merito. Il Responsabile assiste il Titolare, tenendo conto della natura del trattamento e delle informazioni di cui dispone, negli obblighi degli artt. 32-36 GDPR (sicurezza, violazioni, valutazioni d'impatto, consultazione preventiva).

10. Violazioni dei dati

Il Responsabile informa il Titolare senza ingiustificato ritardo, e comunque entro 48 ore da quando ne viene a conoscenza, di ogni violazione dei dati personali che riguarda i dati del Titolare, con le informazioni dell'art. 33, par. 3, GDPR disponibili in quel momento, e le integra appena possibile. L'avviso va all'indirizzo email dell'account del Titolare.

11. Conservazione

- **Contatti:** restano finché il Titolare non li elimina. I contatti eliminati, anche insieme al loro form, sono cancellati definitivamente dopo 30 giorni; così anche il form eliminato con i suoi modelli email, allegati e membri.
- **Contatti oltre il limite mensile del piano** (solo se il limite è attivo, art. 11 delle Condizioni): sono salvati ma restano "in attesa", con il contenuto non visibile al Titolare, finché non rientrano negli invii del mese (al passaggio a un piano superiore o all'inizio del mese successivo, in ordine di arrivo e finché c'è posto). Il Titolare può sempre trovarli (per numero o indirizzo email esatto) ed eliminarli, e li riceve con gli altri dati alla fine del contratto o nel cambio di fornitore. Un contatto in attesa da 90 giorni è cancellato.
- **Registro tecnico delle richieste** (pagina, data e ora, esito, indirizzo IP e browser, account; gli altri dati personali sono oscurati): 90 giorni; 12 mesi per le richieste del personale del Responsabile, perché resti possibile sapere chi ha fatto cosa.
- **Impronte cifrate per i limiti anti-abuso delle email** (indirizzo IP, destinatario, account; mai i dati in chiaro): 2 giorni.
- **Registri degli errori dell'applicazione** (senza i contenuti dei contatti): 30 giorni.
- **Copie di sicurezza** del database: i dati cancellati restano nelle copie fino alla loro scadenza automatica, al massimo 6 mesi; le copie non sono consultabili e servono solo a ripristinare il servizio dopo un guasto.

12. Fine del trattamento

Il Titolare può esportare i propri contatti in qualsiasi momento (art. 14 delle Condizioni). Alla cessazione del contratto, a scelta del Titolare, il Responsabile restituisce i dati, con l'esportazione dell'art. 14 delle Condizioni, oppure li cancella. Il Titolare ha almeno 30 giorni per recuperarli; poi il Responsabile li cancella entro i 30 giorni successivi, salvo gli obblighi di conservazione previsti dalla legge; i dati restano nelle copie di sicurezza fino alla loro scadenza (art. 11). Su richiesta il Responsabile conferma per iscritto la cancellazione.

13. Trasferimenti fuori dallo Spazio economico europeo

I dati sono conservati e trattati nell'Unione europea (Amazon Web Services, Francoforte; per l'invio delle email anche Mailgun, regione UE). Amazon Web Services fa parte di un gruppo statunitense: il suo contratto sul trattamento dei dati prevede le clausole contrattuali tipo della Commissione europea per gli eventuali accessi da fuori dello Spazio economico europeo. I sub-responsabili che possono trattare i dati fuori dallo Spazio economico europeo sono Google (reCAPTCHA) e Mailgun (solo per gli accessi di assistenza dagli Stati Uniti), indicati nell'Allegato A: il trasferimento si basa sulla decisione di adeguatezza UE-USA del 10/07/2023 (Data Privacy Framework), a cui Google LLC e Mailgun Technologies, Inc. hanno aderito, oppure sulle clausole contrattuali tipo.

14. Verifiche e registro dei trattamenti

Il Responsabile mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto del presente Accordo e consente e contribuisce alle verifiche, comprese le ispezioni, svolte dal Titolare o da un revisore da lui incaricato e vincolato alla riservatezza, con un preavviso di almeno 30 giorni, in orario lavorativo e senza accesso ai dati di altri clienti; di regola una volta l'anno, salvo violazioni dei dati o richieste di un'autorità. Le spese della verifica sono a carico del Titolare. Il Responsabile tiene il registro dei trattamenti svolti per conto dei titolari (art. 30, par. 2, GDPR).

15. Modifiche dell'Accordo

Il Responsabile può modificare il presente Accordo per i motivi e con il preavviso dell'art. 9.3 delle Condizioni (almeno 30 giorni, per email e nella dashboard); il Titolare che non è d'accordo può far cessare il contratto senza costi prima che la modifica valga. Le modifiche non riducono il livello di protezione dei dati richiesto dall'art. 28 GDPR.

16. Responsabilità

Ciascuna Parte risponde verso gli interessati secondo l'art. 82 GDPR. Nei rapporti fra le Parti vale l'art. 17 delle Condizioni.

Allegato A — Sub-responsabili

Sub-responsabile	Attività	Dati	Luogo
Amazon Web Services EMEA SARL (Lussemburgo)	Server, database, archiviazione dei file, invio delle email (Amazon SES), registri tecnici	Tutti i dati dei contatti	UE (Francoforte, Germania)
Mailgun (Sinch Email; Mailgun Technologies, Inc. e società del gruppo Sinch)	Invio delle email ai contatti dei form per conto del Titolare (conferme automatiche, risposte dalla dashboard) e delle notifiche dei nuovi contatti	Indirizzo del destinatario, testo dell'email con i valori dei campi, esito della consegna	UE (regione UE di Mailgun); accessi di assistenza dagli USA (art. 13)
Google (reCAPTCHA)	Protezione antispam sui form che la attivano e sulle pagine dei form ospitate dal Responsabile	Indirizzo IP e dati sull'uso della pagina di chi compila; Google tratta questi dati anche come titolare autonomo, secondo le proprie condizioni	UE / USA (art. 13)
Ottimis Group S.r.l., Via del Fontanile Arenato 321, 00163 Roma (RM), P.IVA 14986781004	Segnalazione degli errori tecnici del servizio	Messaggi d'errore, che raramente contengono dati personali (per esempio un indirizzo email in un errore del sistema di posta)	UE (servizio su AWS a Francoforte)

Allegato B — Misure di sicurezza

- Dati conservati e trattati nell'Unione europea; connessioni cifrate (HTTPS).
- Accesso alla dashboard con account personale; password conservate solo come impronta (hash); sessioni chiuse al cambio o al recupero della password; ruoli per singolo form (proprietario, amministratore, editor, lettore).
- Accesso del personale del Responsabile all'account del Titolare solo con credenziali di assistenza, registrato; il personale non può fare dichiarazioni, acquisti o pagamenti al posto del Titolare.
- Registro tecnico delle richieste con i dati personali oscurati e la traccia di chi ha fatto ogni richiesta, compreso il personale del Responsabile; cancellazione automatica (art. 11). Messaggi d'errore ripuliti dall'applicazione prima di essere registrati.
- Protezione dagli invii automatici: campo trappola in tutti i form e, a scelta del Titolare, reCAPTCHA (sempre attivo sulle pagine dei form ospitate).
- Limiti di frequenza sulle email verso indirizzi scelti da chi compila, con impronte cifrate conservate 2 giorni; risposte dalla dashboard solo verso gli indirizzi presenti nel contatto; allegati controllati nel contenuto (tipi ammessi, niente macro né collegamenti esterni).

- File scaricati da indirizzi indicati dagli utenti (per esempio il logo da un link) solo da Internet pubblico, mai dalla rete interna; dashboard non incorporabile in pagine di terzi.
- Aggiornamenti di sicurezza del software applicati appena disponibili per le vulnerabilità critiche.
- Cancellazione automatica dei contatti e dei form eliminati dopo 30 giorni; copie di sicurezza automatiche del database, conservate al massimo 6 mesi.

Documento accettato in modalità telematica tramite la procedura del servizio. Versione 2: sostituisce la versione 1 dal momento in cui il Titolare la accetta. La versione 1 riportava per errore la partita IVA di un'altra società (Ottimis Group S.r.l., 14986781004): quella di Oglut S.r.l. è 15766701005. Le versioni precedenti restano consultabili all'indirizzo form.oglut.com/legal/dpa?v=v1.