Accordo sul trattamento dei dati personali (DPA)

ai sensi dell'art. 28 del Regolamento (UE) 2016/679 — Servizio PrivacyGate · versione 1.0 · 21 settembre 2026 · DPA standard

Parti

TITOLARE DEL TRATTAMENTO
Il Cliente che utilizza il Servizio, identificato nel contratto o nel modulo d'ordine (di seguito, il "Titolare" o il "Cliente")

RESPONSABILE DEL TRATTAMENTO
Innhova di R.M. (ditta individuale), con sede in Via Padule 54, 07024 La Maddalena (SS), P.IVA 02541710907, email privacy@innhova.com (di seguito, "Innhova" o il "Responsabile")

SERVIZIO
La piattaforma software-as-a-service "PrivacyGate" per la gestione degli adempimenti in materia di protezione dei dati personali (registri, richieste degli interessati, violazioni, valutazioni d'impatto, informative, accordi con i partner), fornita da Innhova al Cliente

RESPONSABILE DELLA PROTEZIONE DEI DATI DI INNHOVA
Innhova non ha designato un Responsabile della protezione dei dati (non ricorrono i presupposti dell'art. 37 GDPR); contatto per la privacy: privacy@innhova.com

1 Premessa e definizioni

Il Cliente utilizza il Servizio per gestire dati personali di cui è Titolare e ne affida a Innhova il trattamento in qualità di Responsabile ai sensi dell'art. 28 GDPR. Il presente accordo ("DPA") integra il contratto di fornitura del Servizio (il "Contratto") e ne costituisce parte integrante; in caso di conflitto sui temi della protezione dei dati prevale il DPA.

I termini "dati personali", "trattamento", "titolare", "responsabile", "sub-responsabile", "violazione dei dati personali" e "autorità di controllo" hanno il significato del Regolamento (UE) 2016/679 ("GDPR"). Per "Normativa Privacy" si intende il GDPR, il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e i provvedimenti dell'autorità di controllo.

2 Oggetto, natura, finalità e durata del trattamento

Innhova tratta dati personali per conto di del Cliente al solo fine di erogare il Servizio: ospitare l'istanza dedicata del Cliente, consentire la registrazione, l'archiviazione, la consultazione, l'elaborazione, l'esportazione e la cancellazione dei dati inseriti dal Cliente e dai suoi utenti, garantire sicurezza, continuità e assistenza tecnica.

Le categorie di dati e di interessati sono descritte nell'Allegato I. Il trattamento ha la stessa durata del Contratto e prosegue, limitatamente alla restituzione e alla cancellazione dei dati, secondo l'art. 11.

3 Istruzioni del Titolare

Innhova tratta i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento verso un paese terzo, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetta; in tal caso informa il Titolare prima del trattamento, salvo divieto per rilevanti motivi di interesse pubblico (art. 28.3.a).

Il Contratto, il presente DPA, la documentazione del Servizio e le configurazioni e le operazioni effettuate dal Titolare e dai suoi utenti nel Servizio costituiscono le istruzioni complete e documentate del Titolare. Innhova informa senza ritardo il Titolare se ritiene che un'istruzione violi la Normativa Privacy (art. 28.3, ultimo periodo).

Innhova non tratta i dati per finalità proprie, non li vende e non li utilizza per profilazione, marketing o addestramento di modelli di intelligenza artificiale.

4 Riservatezza e persone autorizzate

Innhova garantisce che le persone autorizzate al trattamento dei dati del Titolare si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (art. 28.3.b), siano formate e operino su istruzioni nel rispetto dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice Privacy. L'accesso ai dati del Titolare è limitato al personale che ne ha necessità per erogare il Servizio o prestare assistenza.

Innhova opera come amministratore di sistema della piattaforma (server, database e applicazione) e osserva il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), come modificato dal Provvedimento del 25 giugno 2009: gli amministratori di sistema sono designati individualmente, con l'elenco degli ambiti di operatività consentiti, dopo la valutazione di esperienza, capacità e affidabilità; l'elenco dei loro estremi identificativi e delle funzioni è tenuto aggiornato e comunicato al Titolare, che lo conserva e può renderlo noto ai propri lavoratori; gli accessi logici sono registrati in registri completi e inalterabili, di cui è verificabile l'integrità, conservati per un periodo non inferiore a sei mesi; l'operato degli amministratori di sistema è verificato almeno una volta l'anno e il Titolare può verificarlo, con la collaborazione di Innhova (art. 12).

5 Misure di sicurezza

Innhova adotta le misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, descritte nell'Allegato II, tenuto conto dello stato dell'arte, dei costi, della natura e dei rischi del trattamento. Le misure sono riesaminate periodicamente e possono essere aggiornate, senza ridurre il livello complessivo di protezione. Il Titolare è responsabile delle misure sui propri sistemi e della gestione delle credenziali dei propri utenti.

6 Sub-responsabili

Il Titolare rilascia un'autorizzazione generale al ricorso ai sub-responsabili elencati nell'Allegato III (art. 28.2 e 28.4). Innhova comunica al Titolare ogni modifica prevista (aggiunta o sostituzione) con almeno 30 giorni di preavviso, all'indirizzo indicato nel Servizio o nel Contratto; entro tale termine il Titolare può opporsi per iscritto e per motivi connessi alla protezione dei dati. Se l'opposizione non può essere risolta in buona fede, il Titolare può recedere dalla parte di Servizio interessata, con rimborso del corrispettivo anticipato per il periodo non goduto.

Innhova stipula con ciascun sub-responsabile un contratto che impone gli stessi obblighi in materia di protezione dei dati previsti dal presente DPA e resta pienamente responsabile verso il Titolare dell'adempimento degli obblighi del sub-responsabile.

7 Trasferimenti di dati verso paesi terzi

Innhova non trasferisce i dati personali del Titolare verso paesi al di fuori dello Spazio Economico Europeo, né consente l'accesso da tali paesi, salvo quanto previsto dall'Allegato III e sempre nel rispetto del Capo V GDPR (decisione di adeguatezza, clausole contrattuali standard o altra garanzia adeguata, con le eventuali misure supplementari).

Le funzioni di intelligenza artificiale del Servizio sono disattivabili dal Titolare e non sono attive di default per la classificazione delle email; se il Titolare le abilita e sceglie un fornitore, i dati inviati al fornitore sono quelli indicati nell'Allegato III e il Titolare ne è informato dal Servizio.

8 Assistenza al Titolare

Tenuto conto della natura del trattamento, Innhova assiste il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, per dare seguito alle richieste degli interessati (artt. 15-22): il Servizio consente al Titolare di estrarre, rettificare, limitare e cancellare i dati. Se Innhova riceve direttamente una richiesta di un interessato, la inoltra al Titolare entro 5 giorni lavorativi e non vi risponde, salvo istruzione contraria.

Innhova assiste inoltre il Titolare nel garantire il rispetto degli obblighi di sicurezza (art. 32), di notifica e comunicazione delle violazioni (artt. 33-34), di valutazione d'impatto e consultazione preventiva (artt. 35-36), fornendo le informazioni ragionevolmente necessarie in suo possesso.

9 Violazioni dei dati personali

Innhova informa il Titolare senza ingiustificato ritardo, e in ogni caso entro 48 ore da quando ne è venuta a conoscenza, di ogni violazione dei dati personali che riguardi i dati del Titolare (art. 33.2). La comunicazione contiene, per quanto noto: la natura della violazione, le categorie e il numero approssimativo di interessati e di registrazioni, le probabili conseguenze, le misure adottate o proposte e un referente per le informazioni.

Innhova collabora con il Titolare per l'analisi, la contenimento e la mitigazione; le comunicazioni all'autorità di controllo e agli interessati restano di competenza del Titolare, salvo diverso accordo scritto.

10 Registro e documentazione

Innhova tiene il registro delle categorie di attività di trattamento svolte per conto del Titolare (art. 30.2), a disposizione dell'autorità di controllo, e mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto degli obblighi del presente DPA.

11 Cessazione del Servizio: restituzione e cancellazione

Alla cessazione del Contratto, per qualunque causa, e su scelta del Titolare comunicata entro 30 giorni, Innhova restituisce i dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico, oppure li cancella. Decorsi 30 giorni dalla cessazione senza indicazioni del Titolare, Innhova cancella i dati.

La cancellazione riguarda l'istanza dedicata (database e file allegati) ed è completata entro 30 giorni dalla richiesta o dalla scadenza del termine; le copie di backup sono eliminate alla naturale scadenza del ciclo di conservazione, comunque non oltre 90 giorni, e nel frattempo non sono utilizzate. Innhova rilascia su richiesta un'attestazione scritta dell'avvenuta cancellazione, salvo che il diritto dell'Unione o nazionale imponga la conservazione dei dati.

12 Verifiche e ispezioni

Innhova mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto del presente DPA e consente e contribuisce alle attività di revisione, comprese le ispezioni, svolte dal Titolare o da un revisore da questi incaricato vincolato a riservatezza (art. 28.3.h). Di norma la verifica avviene con questionari e documentazione; ispezioni in loco o da remoto sono concordate con almeno 30 giorni di preavviso, non più di una volta l'anno, salvo violazione dei dati o richiesta dell'autorità, in orario lavorativo e senza compromettere la sicurezza e la riservatezza dei dati di altri clienti. I costi delle verifiche ulteriori sono a carico del Titolare.

13 Responsabilità

Ciascuna parte risponde secondo l'art. 82 GDPR e nei limiti e alle condizioni previsti dal Contratto, che non possono comunque escludere la responsabilità nei confronti degli interessati né le sanzioni delle autorità di controllo eventualmente comminate a una parte per fatto proprio.

14 Durata, modifiche e legge applicabile

Il DPA entra in vigore alla data di decorrenza del Contratto e resta efficace fino alla completa cancellazione o restituzione dei dati. Innhova può aggiornare il DPA per adeguarlo a modifiche normative o ai provvedimenti delle autorità, con preavviso di 30 giorni; le modifiche sostanziali a svantaggio del Titolare richiedono il suo consenso.

Il DPA è regolato dalla legge italiana e dal GDPR. Per le controversie è competente il Foro di Nola, salvo diversa disposizione inderogabile di legge.

Allegato I — Descrizione del trattamento

Interessati

- Persone che presentano richieste di esercizio dei diritti al Titolare (richiedenti).
- Dipendenti, collaboratori e altri utenti del Titolare che accedono al Servizio (account staff).
- Persone fisiche di cui il Titolare registra i dati nei propri registri: clienti, fornitori e partner (referenti), dipendenti e candidati, segnalanti e segnalati, autorizzati al trattamento e altri soggetti indicati dal Titolare.

Categorie di dati personali

- Dati anagrafici e di contatto (nome, cognome, email, telefono, ruolo, azienda).
- Contenuto delle richieste, delle comunicazioni e dei documenti inseriti o allegati dal Titolare e dai suoi utenti.
- Dati di accesso e di utilizzo del Servizio (identificativi utente, indirizzo IP, data e ora, azioni compiute).
- Dati contenuti nei registri e nelle valutazioni compilati dal Titolare (trattamenti, violazioni, DPIA, accordi), che possono includere, in modo non voluto da Innhova né necessario al Servizio, categorie particolari di dati (art. 9) o dati relativi a condanne penali (art. 10) se il Titolare sceglie di inserirli.

Natura e finalità

- Raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, estrazione, comunicazione al Titolare, limitazione, cancellazione e distruzione, nell’ambito dell’erogazione del Servizio.
- Finalità: consentire al Titolare la gestione della propria conformità alla Normativa Privacy; garantire sicurezza, continuità e assistenza del Servizio.

Durata e localizzazione

- Per la durata del Contratto e fino alla restituzione o cancellazione (art. 11).
- I dati sono ospitati presso Aruba S.p.A. (Aruba Cloud), su infrastruttura situata nello Spazio Economico Europeo.

Allegato II — Misure tecniche e organizzative

Controllo degli accessi e autenticazione

- Ogni cliente dispone di un'istanza con database dedicato e credenziali proprie: i dati di clienti diversi non sono nello stesso database.
- Accesso basato su ruoli (amministratore, DPO, privacy manager, responsabile di reparto, incaricato) e principio del minimo privilegio.
- Password di almeno 12 caratteri con controllo delle password comuni, memorizzate solo come hash con algoritmo bcrypt a costo elevato; blocco temporaneo dell'account dopo tentativi falliti; limitazione della frequenza delle richieste di accesso.
- Verifica in due passaggi: codice monouso via email a validità di 60 secondi oppure app di autenticazione (TOTP); il segreto TOTP è cifrato.
- Configurazione delle funzioni di intelligenza artificiale riservata all'amministratore, con interruttore generale di disattivazione.

Cifratura

- Cifratura in transito con TLS su tutte le connessioni; cookie di sessione con attributi httpOnly, sameSite e secure.
- Cifratura a livello applicativo con AES-256-GCM, con chiave dedicata per ciascun cliente, dei dati degli interessati che presentano richieste (nome, email, telefono, testo delle richieste e dei messaggi), delle chiavi di integrazione, dei segreti di autenticazione e di tutti i file allegati e documenti firmati conservati su disco.
- I registri compilati dal Titolare (trattamenti, violazioni, valutazioni, accordi) sono protetti dall'isolamento per cliente, dal controllo degli accessi e dalla cifratura in transito; [DA CONFERMARE: cifratura del database e del disco a livello di infrastruttura].
- I segreti del tenant (chiave di cifratura dei campi, chiavi di integrazione, password di posta) sono custoditi nel database avvolti con una chiave principale mantenuta fuori dal database: una copia del solo database non consente di leggerli.
- Content-Security-Policy e intestazioni di sicurezza HTTP per la protezione dei browser.

Tracciabilità

- Registro eventi in sola aggiunta (append-only) con catena di hash che rende evidente ogni alterazione: accessi e tentativi falliti, creazione, modifica ed eliminazione dei dati nei registri, esportazioni e download, uso delle funzioni di intelligenza artificiale.
- Il registro non contiene dati personali degli interessati; è conservato per 24 mesi.

Minimizzazione e conservazione

- Il Servizio consente al Titolare di definire periodi di conservazione e di eliminare i dati scaduti, con registro delle cancellazioni.

Continuità, resilienza e verifica

- Backup giornalieri automatici dei database e dei file, cifrati con AES-256, verificati alla creazione e con prova di ripristino mensile; conservati per 30 giorni, con una seconda copia, già cifrata prima del caricamento, su un servizio di archiviazione cloud esterno al server di produzione.
- Aggiornamenti di sicurezza del sistema operativo applicati automaticamente; scansione settimanale delle dipendenze del software alla ricerca di vulnerabilità note, con avviso al responsabile; riavvii pianificati per attivare gli aggiornamenti del sistema.
- [DA CONFERMARE: misure fisiche e di cifratura del disco fornite dal provider di hosting].

Organizzazione

- Personale autorizzato e vincolato a riservatezza; designazione individuale degli amministratori di sistema con registrazione degli accessi.
- Procedura di gestione delle violazioni dei dati con notifica al Titolare entro 48 ore dalla conoscenza.

Allegato III — Sub-responsabili e fornitori

Sub-responsabili autorizzati

- Aruba S.p.A. (Aruba Cloud) — Hosting dell'infrastruttura (server, database e file dell'istanza) — Spazio Economico Europeo
- Google (servizio Google Drive) — Archiviazione della copia esterna dei backup, cifrati con chiave detenuta solo da Innhova prima del caricamento (Google non può leggerne il contenuto) — [DA CONFERMARE: localizzazione dei data center e garanzie di trasferimento]

Servizi scelti o configurati dal Titolare

- Posta elettronica: il Servizio invia e riceve le email tramite il server SMTP/IMAP configurato dal Titolare; tale fornitore è scelto e contrattualizzato dal Titolare.
- Funzioni di intelligenza artificiale (facoltative): se il Titolare le abilita e inserisce la propria chiave di accesso a un fornitore (Anthropic, OpenAI o Google), il Servizio trasmette a tale fornitore il testo necessario alla funzione richiesta (es. la descrizione di un trattamento o il contenuto di una email da classificare). Il Titolare è informato dal Servizio, sceglie il fornitore e ne cura le garanzie per eventuali trasferimenti extra-SEE.
- Servizio di risoluzione dei nomi di dominio (DNS): non tratta dati personali del Titolare.