

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

(Data Processing Agreement — DPA)

ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR)

Versione 3.1 — In vigore dal 05 Febbraio 2026

Parti dell'Accordo

TITOLARE DEL TRATTAMENTO: Il Cliente (Admin, Consulente o Azienda Singola) che utilizza la Piattaforma Green Desk e carica dati personali sulla stessa (di seguito "Titolare").

RESPONSABILE DEL TRATTAMENTO: Leone Ventures S.r.l., Via Stazione, 81013 Piana di Monte Verna (CE), C.F./P.IVA 04892500614, Email: support@leone-ventures.com (di seguito "Responsabile").

Di seguito congiuntamente le "Parti".

Premesse

A. Il Titolare utilizza la piattaforma Green Desk (accessibile all'indirizzo app.greendesk.it) per la gestione di dati relativi alla compliance ambientale aziendale.

B. Nell'ambito dell'erogazione del servizio, il Responsabile tratta dati personali per conto del Titolare in qualità di Responsabile del Trattamento ai sensi dell'art. 28 GDPR.

C. Le Parti intendono regolare con il presente Accordo i termini e le condizioni del trattamento dei dati personali, in conformità all'art. 28, paragrafi 3 e 4, del GDPR.

D. Il presente Accordo costituisce le istruzioni documentate del Titolare al Responsabile ai sensi dell'art. 28, par. 3, lett. a) del GDPR ed è parte integrante delle Condizioni Generali di Servizio della Piattaforma.

Art. 1 — Definizioni

1.1. I termini utilizzati nel presente Accordo hanno il significato attribuito dal GDPR (Regolamento UE 2016/679). In aggiunta:

"Dati Personali": qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4, n. 1, GDPR) caricata o trattata sulla Piattaforma.

"Trattamento": qualsiasi operazione o insieme di operazioni sui Dati Personali, come definita dall'art. 4, n. 2, GDPR.

"Interessato": la persona fisica i cui dati personali sono oggetto di trattamento.

"Violazione dei Dati" (Data Breach): violazione della sicurezza che comporta accidentalmente o illegalmente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati (art. 4, n. 12, GDPR).

"Sub-responsabile": soggetto terzo incaricato dal Responsabile di effettuare specifiche attività di trattamento per conto del Titolare.

Art. 2 — Oggetto, Finalità e Durata del Trattamento

2.1. Il presente Accordo disciplina il trattamento dei Dati Personali effettuato dal Responsabile per conto del Titolare nell'ambito dell'erogazione del servizio Green Desk.

2.2. Finalità del trattamento

Il Responsabile tratta i Dati Personali esclusivamente per le seguenti finalità, su istruzione documentata del Titolare: (a) erogazione del servizio SaaS per la gestione della compliance ambientale; (b) invio di alert automatici via email relativi alle scadenze; (c) assistenza tecnica e supporto; (d) backup, sicurezza e continuità operativa dei dati; (e) audit logging e tracciamento delle operazioni ai fini della sicurezza.

2.3. Natura delle operazioni di trattamento

Raccolta, registrazione, organizzazione, conservazione, consultazione, uso, comunicazione mediante trasmissione, estrazione, messa a disposizione, cancellazione dei Dati Personali, attraverso modalità informatiche e automatizzate.

2.4. Durata del trattamento

Il trattamento ha durata pari al rapporto contrattuale di servizio. Alla cessazione, i dati saranno cancellati o restituiti secondo quanto previsto dall'art. 10, fatti salvi gli obblighi di conservazione previsti dalla legge (fino a 10 anni per obblighi fiscali/legali).

Art. 3 — Tipologie di Dati e Categorie di Interessati

3.1. Tipologie di Dati Personali trattati

Categoria	Dettaglio
Dati identificativi	Nome, cognome, indirizzo email, numero di telefono
Dati aziendali	Ragione sociale, P.IVA, C.F., indirizzi, PEC, codice univoco
Dati di accesso	Credenziali (password in forma crittografata), log di sistema, indirizzi IP, user agent
Dati tecnici	Timestamp di accesso, azioni eseguite, preferenze di notifica
Documenti caricati	Autorizzazioni, prescrizioni, fatture e relativi allegati che possono contenere dati personali

3.2. Categorie di Interessati

Utenti della Piattaforma (Admin, User); legali rappresentanti delle aziende clienti; referenti aziendali indicati nei documenti; eventuali terzi i cui dati siano contenuti nei documenti caricati dagli Utenti.

3.3. Esclusione categorie particolari di dati

Il Titolare dichiara e garantisce di NON caricare sulla Piattaforma categorie particolari di dati di cui all'art. 9 GDPR (dati relativi alla salute, dati genetici, dati biometrici, origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati relativi alla vita sessuale o all'orientamento sessuale) né dati relativi a condanne penali e reati di cui all'art. 10 GDPR. In caso di violazione di tale dichiarazione, il Titolare assume ogni responsabilità e manleva il Responsabile da qualsiasi conseguenza.

Art. 4 — Obblighi del Responsabile

4.1. Il Responsabile si impegna a:

(a) trattare i Dati Personali esclusivamente sulla base delle istruzioni documentate del Titolare (incluso il presente Accordo e le Condizioni Generali di Servizio), salvo che il trattamento sia richiesto dal diritto dell'Unione o dello Stato membro cui è soggetto il Responsabile, nel qual caso il Responsabile informerà il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per motivi di interesse pubblico rilevante;

(b) garantire che le persone autorizzate al trattamento dei Dati Personali si siano impegnate alla riservatezza mediante sottoscrizione di apposito accordo o siano soggette a un obbligo legale di riservatezza di portata adeguata;

(c) adottare tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, conformemente all'art. 32 GDPR, come dettagliato nell'art. 6 del presente Accordo;

(d) rispettare le condizioni per ricorrere a sub-responsabili di cui all'art. 5 del presente Accordo;

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

(f) assistere il Titolare nel rispondere alle richieste degli Interessati relative all'esercizio dei diritti di cui al Capo III del GDPR (artt. 15-22), entro tempi ragionevoli e comunque compatibili con i termini di legge;

(g) su scelta del Titolare, cancellare o restituire tutti i Dati Personali al termine del servizio e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione;

(h) mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente Accordo e all'art. 28 GDPR, e consentire e contribuire alle attività di revisione (audit) e ispezione.

4.2. Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione del Titolare violi il GDPR o altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.

Art. 5 — Sub-responsabili

5.1. Il Titolare autorizza preventivamente e specificamente il ricorso ai seguenti sub-responsabili:

Sub-responsabile	Servizio	Localizzazione	Garanzie
Supabase Inc.	Database PostgreSQL, autenticazione, object storage	UE (AWS Frankfurt / Dublin)	EU-US Data Privacy Framework, SCCs, crittografia AES-256
Vercel Inc.	Hosting e CDN dell'applicazione web	UE / USA (edge network globale)	EU-US Data Privacy Framework, SCCs, SOC 2 Type II
Resend Inc.	Invio email transazionali e notifiche	USA	EU-US Data Privacy Framework, SCCs, crittografia TLS
Hetzner Online GmbH	Esecuzione processi schedulati (cron job) e gestione code email	UE (Germania)	Server UE, ISO 27001, GDPR-compliant, crittografia in transito
Upstash Inc.	Gestione rate limiting, cache e protezione anti-abuso	UE / USA	EU-US Data Privacy Framework, SCCs, SOC 2, crittografia TLS

5.2. Il Responsabile informerà il Titolare di eventuali modifiche relative all'aggiunta o alla sostituzione di sub-responsabili con almeno 30 (trenta) giorni di preavviso, tramite comunicazione email e/o avviso sulla Piattaforma, dando al Titolare la possibilità di opporsi per motivi legittimi entro 15 giorni dalla comunicazione.

5.3. In caso di opposizione giustificata del Titolare, il Responsabile si adopererà per proporre una soluzione alternativa ragionevole. Qualora non sia possibile, il Titolare avrà diritto di recedere dal servizio senza penali.

5.4. Il Responsabile garantisce che ciascun sub-responsabile sia vincolato contrattualmente da obblighi di protezione dei dati non meno stringenti di quelli previsti dal presente Accordo, in conformità all'art. 28, par. 4, GDPR.

5.5. Il Responsabile rimane pienamente responsabile nei confronti del Titolare per l'adempimento degli obblighi dei sub-responsabili.

Art. 6 — Misure di Sicurezza (art. 32 GDPR)

6.1. Il Responsabile adotta e mantiene le seguenti misure tecniche e organizzative, adeguate ai rischi derivanti dal trattamento:

Misure tecniche

Misura	Dettaglio implementativo
Crittografia in transito	HTTPS obbligatorio con TLS 1.3 su tutti gli endpoint
Crittografia a riposo	AES-256 su database e storage (gestita da Supabase/AWS)

Autenticazione sicura	Password policy con requisiti minimi di complessità (minimo 8 caratteri), token di sessione con scadenza, protezione brute force con rate limiting (5 tentativi/minuto), protezione anti-enumerazione account
Isolamento multi-tenant	Architettura a compartimenti stagni: ogni Organization ha dati logicamente isolati, verificati a livello applicativo su ogni query (checkCompanyAccess)
Controllo accessi (RBAC)	Role-Based Access Control a 3 livelli (SuperAdmin, Admin, User) con principio del minimo privilegio
Backup automatici	Backup giornalieri automatici gestiti da Supabase con retention adeguata
Audit trail	Log immutabili di tutte le operazioni CRUD con timestamp, actor, IP, dati precedenti e successivi. Trigger DB impediscono modifica/cancellazione dei log
Rate limiting	Protezione endpoint critici con Upstash Redis (login, reset password, inviti, upload, operazioni CRUD)
Sanitizzazione input	Validazione lato server con Zod, escape HTML per prevenzione XSS, sanitizzazione nomi file per prevenzione path traversal

Misure organizzative

Accesso ai dati limitato al personale strettamente necessario (principio di need-to-know); obbligo di riservatezza per tutto il personale autorizzato; procedure documentate di incident response; revisione periodica delle misure di sicurezza; formazione del personale in materia di protezione dei dati.

6.2. Il Responsabile si impegna a riesaminare periodicamente le misure di sicurezza e ad aggiornarle in funzione dell'evoluzione tecnologica, dei rischi e delle best practice di settore.

Art. 7 — Trasferimenti Extra-UE

7.1. I dati primari del Titolare sono conservati su server situati nell'Unione Europea (regione AWS Frankfurt, Germania, e/o Dublin, Irlanda).

7.2. I trasferimenti di dati verso sub-responsabili situati negli Stati Uniti d'America avvengono sulla base di: (a) Decisione di adeguatezza della Commissione Europea per il EU-US Data Privacy Framework (Decisione C(2023) 4745 del 10 luglio 2023), per i soggetti certificati; (b) Clausole Contrattuali Standard (SCCs) approvate dalla Commissione Europea con Decisione di Esecuzione (UE) 2021/914, come misura supplementare.

7.3. Il Responsabile garantisce che non verranno effettuati trasferimenti di Dati Personali verso paesi terzi in assenza di adeguate garanzie ai sensi del Capo V del GDPR. In caso di invalidazione del meccanismo di trasferimento utilizzato, il Responsabile ne darà tempestiva comunicazione al Titolare e adotterà le misure supplementari necessarie.

7.4. Il Titolare può richiedere informazioni aggiuntive sulle garanzie per i trasferimenti Extra-UE scrivendo a support@leone-ventures.com.

Art. 8 — Notifica delle Violazioni (Data Breach)

8.1. In caso di Violazione dei Dati Personali di cui venga a conoscenza, il Responsabile notificherà il Titolare senza ingiustificato ritardo e comunque entro 24 (ventiquattro) ore dalla scoperta o dalla ragionevole certezza della violazione.

8.2. La notifica conterrà almeno: (a) descrizione della natura della violazione, incluse, ove possibile, le categorie e il numero approssimativo di Interessati coinvolti e di registrazioni di dati personali interessate; (b) nome e recapiti del punto di contatto del Responsabile; (c) descrizione delle probabili conseguenze della violazione; (d) descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

8.3. Il Responsabile collaborerà attivamente con il Titolare per la gestione della violazione e l'eventuale notifica al Garante per la Protezione dei Dati Personali (entro 72 ore dalla conoscenza ai sensi dell'art. 33 GDPR) e agli Interessati (ai sensi dell'art. 34 GDPR).

8.4. Il Responsabile documenterà qualsiasi Violazione dei Dati Personali, comprese le circostanze, le conseguenze e i provvedimenti adottati, mettendo tale documentazione a disposizione del Titolare e dell'autorità di controllo su richiesta.

Art. 9 — Assistenza al Titolare

9.1. Il Responsabile assiste il Titolare: (a) nel rispondere alle richieste degli Interessati relative all'esercizio dei diritti di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione) entro i termini di legge; (b) nella conduzione di valutazioni d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 GDPR, quando richiesto; (c) nell'eventuale consultazione preventiva con il Garante ai sensi dell'art. 36 GDPR.

9.2. L'assistenza sarà fornita tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile, nei limiti di quanto tecnicamente fattibile e ragionevolmente esigibile.

Art. 10 — Restituzione e Cancellazione dei Dati

10.1. Al termine del rapporto contrattuale, su scelta del Titolare comunicata per iscritto entro 30 (trenta) giorni dalla cessazione, il Responsabile: (a) restituirà tutti i Dati Personali al Titolare nei formati tecnicamente disponibili (export CSV, PDF, ZIP); oppure (b) cancellerà tutti i Dati Personali e le copie esistenti.

10.2. In assenza di istruzioni del Titolare entro il termine di cui sopra, il Responsabile procederà alla cancellazione dei dati.

10.3. Il Responsabile potrà conservare copie dei Dati Personali esclusivamente nella misura in cui la conservazione sia imposta dal diritto dell'Unione o dello Stato membro, dandone comunicazione al Titolare e garantendo la riservatezza dei dati conservati.

Art. 11 — Audit e Verifiche

11.1. Il Responsabile mette a disposizione del Titolare la documentazione necessaria a dimostrare il rispetto degli obblighi di cui al presente Accordo e all'art. 28 GDPR.

11.2. Il Titolare (o un revisore indipendente da questi incaricato, vincolato da obblighi di riservatezza) può effettuare verifiche e ispezioni, previo accordo scritto con ragionevole preavviso (almeno 30

giorni), nel rispetto degli obblighi di riservatezza del Responsabile e senza interferire con le normali attività operative.

11.3. I costi delle verifiche sono a carico del Titolare, salvo che la verifica evidenzi inadempimenti del Responsabile agli obblighi del presente Accordo.

11.4. Le verifiche non potranno avere ad oggetto dati di altri clienti del Responsabile (principio di compartimenti stagni) e saranno limitate ai dati e ai trattamenti di pertinenza del Titolare.

Art. 12 — Responsabilità

12.1. Ciascuna Parte è responsabile dei danni causati dal trattamento che violi il GDPR, nei limiti e alle condizioni previste dall'art. 82 GDPR.

12.2. Il Responsabile è esonerato dalla responsabilità ai sensi dell'art. 82, par. 3, GDPR se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

12.3. La responsabilità del Responsabile per danni derivanti dal presente Accordo è soggetta alla limitazione massima prevista dall'art. 6.4 delle Condizioni Generali di Servizio (cap pari ai corrispettivi pagati nei 12 mesi precedenti), fermo restando quanto previsto da norme inderogabili di legge.

Art. 13 — Durata e Disposizioni Finali

13.1. Il presente Accordo ha la stessa durata del contratto di servizio sottostante e si risolve automaticamente alla cessazione del medesimo.

13.2. Gli obblighi di riservatezza e le disposizioni relative alla restituzione/cancellazione dei dati sopravvivono alla cessazione del presente Accordo.

13.3. Il presente Accordo è regolato dalla legge italiana e dal GDPR.

13.4. Per quanto non espressamente previsto, si applicano le disposizioni del GDPR, del contratto di servizio e delle Condizioni Generali di Servizio.

13.5. In caso di conflitto tra il presente Accordo e altri documenti contrattuali, prevalgono le disposizioni del presente Accordo in materia di protezione dei dati personali.

Allegato — Istruzioni Documentate del Titolare

Il Titolare fornisce le seguenti istruzioni al Responsabile per il trattamento dei Dati Personali:

1. Trattare i dati esclusivamente per l'erogazione del servizio Green Desk e le finalità di cui all'art. 2.2.
2. Non utilizzare i dati per finalità proprie, di marketing o profilazione del Responsabile.
3. Non cedere, comunicare o rendere accessibili i dati a terzi non autorizzati.

4. Conservare i dati primari sui server nell'Unione Europea come indicato all'art. 7.
5. Applicare e mantenere le misure di sicurezza descritte all'art. 6.
6. Notificare tempestivamente eventuali violazioni secondo le modalità dell'art. 8.
7. Assistere il Titolare nelle richieste degli Interessati secondo le modalità dell'art. 9.
8. Restituire o cancellare i dati al termine del servizio secondo le modalità dell'art. 10.
9. Garantire l'immutabilità e la disponibilità degli audit log per la durata del rapporto.

— *Fine del Documento* —