Nomina Responsabile del Trattamento

Atto di nomina ai sensi dell'Art. 28 del Regolamento UE 2016/679 — parte integrante del contratto di servizio CRM Trasporti.

A chi è destinato questo documento
Il presente atto regola il trattamento dei dati personali effettuato da DANIELE LILLA CONSULTING, in qualità di Responsabile, per conto del Cliente del servizio CRM Trasporti, in qualità di Titolare. È parte integrante del contratto SaaS sottoscritto dal Cliente.

Premesse

Visto che il Cliente (di seguito anche "Titolare"), aderendo al servizio SaaS CRM Trasporti, conferisce a **DANIELE LILLA CONSULTING**, P. IVA 03224870596, con sede in Via Giuseppe Verdi, 110, 04017 San Felice Circeo (LT) (di seguito "Responsabile" o "Fornitore"), l'incarico di effettuare alcuni trattamenti di dati personali per suo conto;

Considerato che ai sensi dell'Art. 28 del Regolamento UE 2016/679 (GDPR), il Titolare deve nominare formalmente il Responsabile del Trattamento e regolarne compiti, garanzie e obblighi;

Tutto ciò premesso e considerato, il Cliente nomina **DANIELE LILLA CONSULTING** Responsabile del Trattamento ai sensi dell'Art. 28 GDPR, alle condizioni di seguito specificate.

1. Oggetto e durata della nomina

1.1 La nomina ha per oggetto i trattamenti effettuati dal Responsabile per fornire il servizio CRM Trasporti (autenticazione, archiviazione, elaborazione, backup, comunicazioni di servizio, supporto tecnico, fatturazione elettronica via SDI, invio notifiche).

1.2 La nomina ha la stessa durata del contratto di servizio. Decorso il contratto, il Responsabile cessa ogni operazione di trattamento, salvi gli obblighi di restituzione/cancellazione previsti all'art. 8.

2. Natura del trattamento

Categorie di interessati

- Dipendenti, soci, autisti del Titolare (azienda Cliente)
- Clienti / committenti del Titolare (anagrafiche commerciali)
- Fornitori del Titolare (officine, fuel card, ecc.)
- Eventuali altri soggetti i cui dati siano caricati dal Titolare nel software

Categorie di dati personali

- Dati identificativi e di contatto (nome, email, telefono, indirizzo)
- Dati fiscali (P.IVA, codice fiscale, IBAN)
- Dati relativi al rapporto di lavoro degli autisti (patente, CQC, ADR, contratti, scadenze sanitarie)
- Dati relativi a viaggi e operatività (geolocalizzazione, orari, percorsi, foto)
- Dati operativi della flotta (targhe, telai, libretti)
- File tachigrafo digitale (.DDD/C1B)
- Documenti di trasporto (DDT, CMR), firmati e foto
- Fatture, pagamenti, scadenziari
- Eccezionalmente, dati relativi a salute (visite mediche autisti), categoria particolare ex Art. 9 GDPR

Operazioni di trattamento

Raccolta, registrazione, organizzazione, strutturazione, archiviazione, adattamento, estrazione, consultazione, uso, comunicazione mediante trasmissione, raffronto, limitazione, cancellazione, distruzione.

3. Obblighi del Responsabile

Ai sensi dell'Art. 28.3 GDPR, il Responsabile si obbliga a:

a) trattare i dati personali esclusivamente su istruzione documentata del Titolare, ivi inclusi i casi di trasferimento extra-UE, salvo che lo richieda il diritto dell'Unione o nazionale; in tal caso il Responsabile informa il Titolare prima del trattamento, salvo divieto di legge;

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 tecniche e organizzative adeguate ai sensi dell'Art. 32 GDPR (vedi art. 4 del presente atto);

d) rispettare le condizioni per ricorrere a sub-responsabili (vedi art. 5 del presente atto);

e) assistere il Titolare con misure tecniche e organizzative appropriate, nella misura possibile, per consentirgli di soddisfare le richieste degli interessati ex Artt. 15–22 GDPR;

f) assistere il Titolare nel rispetto degli obblighi di sicurezza, notifica violazioni, valutazione d'impatto e consultazione preventiva (Artt. 32–36 GDPR);

g) su richiesta del Titolare, cancellare o restituire tutti i dati personali al termine del contratto (vedi art. 8);

h) mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi ex Art. 28 GDPR e consentire/contribuire ad audit, anche tramite ispezioni, da parte del Titolare o di un soggetto da questi incaricato.

4. Misure di sicurezza (Art. 32 GDPR)

Il Responsabile dichiara di aver adottato le seguenti misure tecniche e organizzative:

4.1 Misure tecniche

Crittografia in transito: TLS 1.2/1.3 su tutti i canali web e API

Crittografia a riposo: database PostgreSQL cifrato; campi sensibili (CF, IBAN, dati salute) cifrati con AES-256-GCM e chiave dedicata

Hashing password: bcrypt con work factor ≥ 12

Multi-Factor Authentication: opzionale ma consigliata, TOTP (RFC 6238)

Isolamento multi-tenant: doppio livello — Row Level Security (RLS) lato database + middleware applicativo. Anche un eventuale bug del codice non consente a un tenant di leggere dati di un altro tenant

Audit log immutabili: tracciamento di accessi, modifiche e operazioni sensibili

Backup automatici: orari e giornalieri, cifrati, in regione UE separata, con test di restore mensile

Hardening server: firewall (ufw), fail2ban, aggiornamenti automatici di sicurezza, no root login, accesso SSH solo con chiave ed25519

Web Application Firewall tramite Cloudflare

Headers di sicurezza HTTP: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy

Soft delete con retention: i dati cancellati sono mascherati per 24 mesi prima della cancellazione definitiva, salvo obblighi di conservazione fiscale (10 anni per fatture)

4.2 Misure organizzative

Accesso ai sistemi consentito solo a personale formalmente autorizzato e formato sulla protezione dati

Vincolo di riservatezza scritto per tutti i collaboratori

Procedura interna di gestione data breach

Registro dei trattamenti aggiornato (Art. 30 GDPR)

Penetration test annuale a partire dal primo anno operativo

Revisione periodica delle misure di sicurezza

4.3 Localizzazione dei dati

I dati personali sono ospitati esclusivamente in Unione Europea. Datacenter principale: Germania (Falkenstein). Datacenter backup/disaster recovery: Germania (Norimberga) o Finlandia (Helsinki).

Eventuali servizi accessori che operano da paesi extra-UE (Cloudflare USA per CDN, Stripe USA per pagamenti) operano in regime di Standard Contractual Clauses (SCC) approvate dalla Commissione Europea, integrate da misure supplementari ove opportuno.

5. Sub-responsabili

5.1 Il Titolare autorizza in via generale il Responsabile a ricorrere ai seguenti sub-responsabili per l'erogazione del servizio:

Sub-responsabile	Servizio	Sede
Hetzner Online GmbH	Hosting cloud, archiviazione	Germania (UE)
Cloudflare, Inc.	DNS, CDN, mitigazione DDoS, WAF	USA (SCC + DPF)
Stripe Payments Europe Ltd	Elaborazione pagamenti	Irlanda (UE)
Resend Inc. / Postmark	Email transazionali	USA (SCC + DPF)
Acube S.r.l. (futuro)	Invio fatture SDI	Italia
Make.com (Celonis SE)	Automazione form contatti del sito vetrina	Germania (UE)
Google Document AI (futuro)	OCR DDT/CMR, solo per clienti che attivano la feature	UE (regione europea)

5.2 Tutti i sub-responsabili sono vincolati da contratti di Data Processing Agreement che impongono obblighi equivalenti a quelli della presente nomina, in particolare in materia di sicurezza (Art. 32) e violazioni (Art. 33).

5.3 Il Responsabile informerà il Titolare di eventuali modifiche all'elenco dei sub-responsabili con preavviso di almeno 30 giorni, dando al Titolare la possibilità di opporsi (con conseguente diritto di recesso senza penali in caso di modifica essenziale).

6. Notifica violazioni dei dati personali (Art. 33 GDPR)

In caso di violazione dei dati personali (data breach), il Responsabile ne informa il Titolare **senza ingiustificato ritardo, e comunque entro 48 ore** dalla scoperta, fornendo:

- la natura della violazione (categorie e numero approssimativo di interessati e dati coinvolti);
- nome e contatti del referente;
- conseguenze probabili della violazione;
- misure adottate o proposte per porvi rimedio.

Resta in capo al Titolare l'obbligo di notifica al Garante entro 72 ore (Art. 33) e agli interessati (Art. 34) ove applicabile.

7. Audit e ispezioni

7.1 Il Titolare ha il diritto di verificare la conformità del Responsabile, mediante:

- richiesta scritta di documentazione (politiche di sicurezza, certificazioni, report di pen test sintetici);
- eventuale audit in sede, previa pianificazione concordata (con almeno 30 giorni di preavviso, salvo violazione grave) e a spese del Titolare.

7.2 In alternativa, il Responsabile può fornire un report di audit indipendente effettuato da terzi qualificati (es. SOC 2, ISO 27001 quando disponibile).

8. Restituzione/cancellazione dei dati

8.1 Al termine del contratto, su scelta del Titolare, il Responsabile:

- consegna al Titolare un'esportazione completa dei dati in formato strutturato (CSV/Excel/XML/PDF), entro 30 giorni dalla richiesta; oppure
- cancella tutti i dati personali del Titolare entro 30 giorni dalla cessazione del contratto, salvo diversi obblighi di conservazione previsti dalla legge (es. fatture: 10 anni).

8.2 Il Responsabile fornisce conferma scritta dell'avvenuta cancellazione.

9. Trasferimenti extra-UE

Eventuali trasferimenti verso paesi terzi avvengono esclusivamente con le garanzie ex Artt. 45-46 GDPR (decisioni di adeguatezza, Standard Contractual Clauses), come specificato all'art. 4.3 e all'art. 5.1 del presente atto.

10. Comunicazioni

10.1 Le comunicazioni relative al presente atto sono inviate ai seguenti recapiti del Responsabile:
Email: privacy@crmtrasporti.com
PEC:

10.2 Le comunicazioni del Responsabile al Titolare sono inviate all'email comunicata in fase di registrazione.

11. Foro competente

Per ogni controversia relativa al presente atto, sarà competente in via esclusiva il Foro di LT (San Felice Circeo).

12. Accettazione

Il presente Atto di Nomina viene accettato dal Titolare al momento della sottoscrizione del contratto di servizio, di cui costituisce allegato e parte integrante.

Documento collegato: Termini e Condizioni del servizio · Informativa Privacy · Allegato Tecnico

Atto redatto dal Responsabile DANIELE LILLA CONSULTING (Daniele Lilla, REA LT - 315488). Ultimo aggiornamento: maggio 2026.

Hai bisogno di un DPA standard sottoscritto separatamente dalla tua azienda?

Smetti di rincorrere fatture e scadenze.

Prenota una demo gratuita: ti mostriamo il gestionale dal vivo, anche sui tuoi dati. Nessun impegno.

Chiama subito | Prenota una demo

CT CRM TRASPORTI

Il gestionale italiano per chi guida un'azienda di autotrasporto. Viaggi, mezzi, autisti, fatture e scadenze in un unico posto. Niente più Excel.

L'app è disponibile su App Store e Google Play, ma non è obbligatoria: si lavora anche solo dal browser, e all'autista il viaggio arriva su WhatsApp o su carta.

Scarica su App Store | DISPONIBILE SU Google Play

PRODOTTO

- Funzionalità
- Soluzioni
- Settori
- Prezzi
- Guide
- Glossario
- Demo gratuita
- Allegato Tecnico
- Accedi al Gestionale

AZIENDA

- Chi Siamo
- Contatti
- Privacy Policy
- Termini e Condizioni
- Cookie Policy

CONTATTI

info@crmtrasporti.com

Via Giuseppe Verdi, 110
04017 San Felice Circeo (LT)

Dati cifrati, backup ogni ora

Nomina Trattamento Dati

Conformi al GDPR

Sede: Via Giuseppe Verdi, 110, 04017 San Felice Circeo (LT)