DANIELE LILLA CONSULTING

Nomina a Responsabile del trattamento

Atto di nomina ai sensi dell'articolo 28 del Regolamento UE 2016/679, parte integrante e sostanziale del contratto di servizio CRM Trasporti

IDENTIFICAZIONE DEL DOCUMENTO	
Versione	1.1
In vigore dal	10.08.2026
Sostituisce	versione 1.0 del 15.05.2026

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

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 e cancellazione previsti all'art. 14 del presente atto.

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 e diritti del Titolare

Ai sensi dell'articolo 28, paragrafo 3, del Regolamento, che richiede la determinazione contrattuale degli obblighi e dei diritti del titolare del trattamento, le Parti convengono quanto segue.

Obblighi del Titolare

Il Titolare si obbliga a:

- trattare i dati personali nel rispetto dei principi di cui all'articolo 5 del Regolamento, verificando la sussistenza di una **base giuridica idonea** per ciascuna finalità perseguita mediante la piattaforma;
- rendere agli interessati le **informative** di cui agli articoli 13 e 14 del Regolamento, dandone evidenza su richiesta del Responsabile;
- impartire al Responsabile **istruzioni lecite, documentate e non eccedenti** rispetto alle finalità dichiarate, anche mediante le configurazioni operate nella piattaforma, che costituiscono a tutti gli effetti istruzioni documentate;
- inserire e mantenere aggiornati dati **esatti, pertinenti e limitati** a quanto necessario, astenendosi dall'immettere categorie di dati non previste dall'Allegato relativo alla natura del trattamento;
- adempiere, ove il trattamento comporti la possibilità di controllo a distanza dell'attività dei lavoratori, agli obblighi previsti dall'**articolo 4 della Legge 300/1970** prima dell'attivazione delle relative funzionalità;
- effettuare, ove ricorrano i presupposti dell'articolo 35 del Regolamento, la **valutazione d'impatto** sulla protezione dei dati, avvalendosi delle informazioni messe a disposizione dal Responsabile;
- tenere il **registro delle attività di trattamento** di cui all'articolo 30, paragrafo 1, del Regolamento;
- custodire le credenziali di accesso, gestire le abilitazioni dei propri utenti e revocarle tempestivamente al cessare dei presupposti;
- comunicare senza indugio al Responsabile ogni circostanza rilevante ai fini del trattamento, ivi comprese le variazioni dei recapiti, del legale rappresentante e del referente per la protezione dei dati;
- dare riscontro alle richieste del Responsabile relative all'esecuzione del presente atto entro termini congrui e comunque non superiori a quindici giorni.

Diritti del Titolare

Il Titolare ha diritto di:

- impartire in ogni momento **istruzioni ulteriori o modificative** in forma scritta, purché compatibili con le caratteristiche tecniche del servizio; ove l'istruzione richieda adeguamenti tecnici, le Parti concordano tempi e modalità di attuazione ed eventuali corrispettivi;
- ottenere dal Responsabile **tutte le informazioni necessarie** a dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento;
- effettuare **verifiche e ispezioni** con le modalità previste dal presente atto;
- essere **informato preventivamente** di ogni variazione dell'elenco dei sub-responsabili e opporsi per motivi ragionevoli e documentati;
- ottenere, alla cessazione del rapporto, la **restituzione o la cancellazione** dei dati secondo la scelta espressa;

- ottenere l'**assistenza** del Responsabile per dare seguito alle richieste degli interessati e per gli adempimenti di cui agli articoli da 32 a 36 del Regolamento;
- consultare il **registro degli accessi** effettuati dal Responsabile per finalità di assistenza;
- opporsi ai trattamenti ulteriori autorizzati relativi alle statistiche d'uso e alle elaborazioni aggregate.

Responsabilità del Titolare per le istruzioni impartite

Il Responsabile non risponde delle conseguenze derivanti dall'esecuzione di istruzioni impartite dal Titolare, salvo il caso in cui abbia omesso di segnalarne la manifesta illegittimità ai sensi del presente atto. Restano a carico del Titolare le conseguenze derivanti dall'assenza di una base giuridica idonea, dalla mancata informativa agli interessati e dall'inosservanza degli obblighi previsti dall'articolo 4 della Legge 300/1970.

4 — 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. 6 del presente atto);

d) rispettare le condizioni per ricorrere a sub-responsabili (vedi art. 8 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. 14 del presente atto);

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.

5 — Ulteriori obblighi del Responsabile

Segnalazione delle istruzioni illegittime. Ai sensi dell'art. 28, paragrafo 3, secondo capoverso, del GDPR, il Responsabile informa immediatamente il Titolare qualora ritenga che una sua istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, sospendendo l'esecuzione dell'istruzione fino a diverso avviso del Titolare.

Persone autorizzate al trattamento. Il Responsabile designa per iscritto, ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, le persone fisiche autorizzate al trattamento, impartisce loro istruzioni documentate, ne verifica periodicamente l'operato e provvede alla revoca delle autorizzazioni al cessare dei presupposti. Le persone autorizzate sono vincolate a un obbligo di riservatezza che permane anche dopo la cessazione del rapporto.

Registro dei trattamenti. Il Responsabile tiene il registro delle categorie di attività di trattamento svolte per conto del Titolare ai sensi dell'art. 30, paragrafo 2, del GDPR, e lo mette a disposizione dell'autorità di controllo su richiesta.

Richieste dell'autorità. Qualora il Responsabile riceva da un'autorità giudiziaria, di polizia o amministrativa una richiesta di accesso, esibizione o comunicazione dei dati trattati per conto del Titolare, ne informa senza indugio il Titolare, salvo che ciò sia vietato dalla legge, e fornisce esclusivamente i dati strettamente indicati nella richiesta.

Richieste degli interessati. Qualora il Responsabile riceva direttamente da un interessato una richiesta di esercizio dei diritti di cui agli artt. 15-22 del GDPR relativa a dati trattati per conto del Titolare, si astiene dal darvi seguito autonomamente e la trasmette al Titolare entro cinque giorni lavorativi, assistendolo con misure tecniche e organizzative appropriate.

6 — Misure di sicurezza (art. 32 GDPR)

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

6.1 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: scrypt (N = 16384, r = 16, p = 1) con sale per utente; le password non sono mai conservate in chiaro né reversibili
- 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
- Cancellazione logica e cancellazione definitiva: la cancellazione richiesta dall'utente rende il dato immediatamente inaccessibile nella piattaforma; la cancellazione definitiva dagli ambienti di produzione avviene nei termini dell'art. 14 del presente atto, e la permanenza nelle copie di sicurezza segue l'art. 15 del presente atto, salvi gli obblighi di conservazione fiscale (dieci anni per le fatture)

6.2 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

6.3 Localizzazione dei dati

I dati del Titolare sono archiviati esclusivamente su datacenter ubicati nell'Unione Europea. Datacenter principale: Germania (Falkenstein). Datacenter backup/disaster recovery: Germania (Norimberga) o Finlandia (Helsinki).

Alcuni servizi accessori comportano trasferimenti verso Paesi terzi: sono i sub-responsabili indicati con sede negli Stati Uniti nell'elenco dell'art. 8 del presente atto. Tali trasferimenti operano in regime di Clausole Contrattuali Tipo approvate dalla Commissione europea, integrate da misure supplementari ove opportuno e, ove applicabile, dalla decisione di adeguatezza relativa al Data Privacy Framework UE-Stati Uniti.

7 — Accesso del Responsabile per finalità di assistenza

Il Titolare autorizza il Responsabile ad accedere ai dati oggetto del trattamento esclusivamente per: erogare l'assistenza tecnica richiesta dal Titolare o dai suoi utenti; diagnosticare e risolvere malfunzionamenti della piattaforma; garantire la sicurezza dei sistemi. L'accesso è consentito al solo personale designato ai sensi dell'art. 29 del GDPR, è limitato a quanto strettamente necessario ed è articolato su livelli progressivi:

- **diagnostica**: accesso ai soli metadati tecnici, registri di errore e indicatori di funzionamento, senza accesso al contenuto dei dati;

- **assistenza**: accesso in sola lettura ai dati del Titolare, previa richiesta di quest'ultimo o apertura di una segnalazione;
- **intervento**: accesso in lettura e scrittura, previa motivazione documentata e limitatamente alla durata dell'intervento.

Ogni accesso ai livelli di assistenza e intervento è integralmente registrato in un giornale di controllo immutabile riportante identità dell'operatore, data e ora di inizio e fine, ambito dell'accesso e motivazione. Le sessioni di accesso hanno durata limitata e decadono automaticamente. **Il Titolare può consultare in ogni momento il registro degli accessi dalla propria area riservata.**

8 — Sub-responsabili

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

Sub-responsabile	Servizio affidato	Sede	Garanzia per il trasferimento
Hetzner Online GmbH	Hosting cloud e archiviazione dei dati	Germania	Territorio UE
Cloudflare, Inc.	DNS, rete di distribuzione dei contenuti, mitigazione DDoS, web application firewall	Stati Uniti	SCC + DPF
Stripe Payments Europe Ltd	Elaborazione dei pagamenti	Irlanda	Territorio UE
Resend Inc.	Invio di messaggi di posta elettronica transazionali	Stati Uniti	SCC + DPF
Make.com (Celonis SE)	Automazione dei moduli di contatto del sito istituzionale	Germania	Territorio UE
LogRocket, Inc.	Registrazione delle sessioni di navigazione sul sito istituzionale. Non attivo nell'ambiente applicativo	Stati Uniti	SCC
Acube S.r.l.	Trasmissione delle fatture elettroniche al Sistema di Interscambio (in attivazione)	Italia	Territorio UE
Google Ireland Ltd	Riconoscimento ottico dei caratteri su documenti di trasporto, limitatamente ai Clienti che attivano la funzionalità	Irlanda	Territorio UE

8.2 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).

8.3 Il Responsabile informa il Titolare di ogni modifica dell'elenco dei sub-responsabili con preavviso di almeno trenta giorni, entro il quale il Titolare può opporsi per motivi ragionevoli e documentati, con diritto di recesso senza penalità limitatamente ai servizi interessati. L'elenco aggiornato è pubblicato e consultabile alla pagina crmtrasporti.com/legal/sub-responsabili.

9 — Trasferimenti verso Paesi terzi

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. 6.3 e all'art. 8.1 del presente atto.

10 — 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 24 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.

11 — Verifiche e ispezioni

11.1 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.

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

12 — Trattamenti ulteriori autorizzati dal Titolare

Il Titolare autorizza il Responsabile a effettuare i seguenti trattamenti, riconducibili alle finalità di erogazione e miglioramento del servizio:

- rilevazione di **statistiche d'uso** della piattaforma, riferite alle modalità e alla frequenza di utilizzo delle funzionalità, alle prestazioni e agli errori, e non al contenuto dei dati;
- elaborazione di **informazioni aggregate e anonime** per finalità statistiche, di analisi di mercato e di miglioramento del servizio, a condizione che il risultato non sia riconducibile al Titolare, ai suoi clienti o fornitori né ad alcun interessato, e che ciascuna elaborazione sia calcolata su un numero minimo di soggetti distinti e con un limite al contributo del singolo soggetto, secondo le soglie indicate nell'Allegato Tecnico;
- trattamenti necessari alla **sicurezza informatica**, alla prevenzione delle frodi e alla diagnosi dei malfunzionamenti.

È escluso ogni ulteriore trattamento per finalità proprie del Responsabile. In particolare, il Responsabile non utilizza i dati del Titolare per attività di marketing, per la creazione di segmenti di pubblico pubblicitari, per la profilazione di soggetti terzi, né per contattare clienti, fornitori o committenti del Titolare. Nell'area applicativa non sono installati strumenti di profilazione o di tracciamento pubblicitario di terze parti.

Il Titolare può opporsi ai trattamenti di cui ai primi due punti mediante comunicazione all'indirizzo privacy@crmtrasporti.com.

13 — Geolocalizzazione e controllo a distanza

Con riferimento ai dati di posizione dei veicoli e ai dati estratti dal tachigrafo digitale, il Titolare dichiara di aver adempiuto agli obblighi previsti dall'**art. 4 della Legge 20 maggio 1970, n. 300**, come modificato dall'art. 23 del D.Lgs. 151/2015, mediante stipula di accordo collettivo con le rappresentanze sindacali ovvero, in mancanza, previa autorizzazione della competente sede dell'Ispettorato nazionale del lavoro, e di aver reso ai lavoratori l'informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli prevista dal comma 3 del medesimo articolo, condizione di utilizzabilità dei dati raccolti a ogni fine connesso al rapporto di lavoro.

Il Responsabile mette a disposizione del Titolare le funzioni di configurazione descritte nelle Condizioni Particolari, la cui impostazione in conformità agli obblighi di legge resta di esclusiva competenza del Titolare.

14 — Restituzione e cancellazione dei dati

14.1 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).

14.2 Il Responsabile fornisce conferma scritta dell'avvenuta cancellazione.

14.3 Le richieste di cancellazione degli interessati ai sensi dell'art. 17 del GDPR sono eseguite dal Responsabile, su istruzione del Titolare, senza ingiustificato ritardo, salvi i casi in cui la conservazione sia imposta da un obbligo di legge; la permanenza dei dati nelle copie di sicurezza è disciplinata dall'art. 15 del presente atto.

15 — Cancellazione dalle copie di sicurezza

La cancellazione dei dati dagli ambienti di produzione non comporta la contestuale cancellazione dalle copie di sicurezza, che seguono il ciclo di rotazione indicato nell'Allegato Tecnico. Fino alla sovrascrittura, i dati presenti nelle copie di sicurezza non sono oggetto di alcun trattamento ulteriore e restano protetti dalle misure di sicurezza previste dal presente atto.

16 — Durata degli obblighi

Gli obblighi di riservatezza e di sicurezza previsti dal presente atto permangono anche dopo la cessazione del contratto, per tutto il tempo in cui il Responsabile conservi, anche solo su supporti di backup, dati trattati per conto del Titolare.

17 — Comunicazioni

17.1 Le comunicazioni relative al presente atto sono inviate ai seguenti recapiti del Responsabile: email privacy@crmtrasporti.com, PEC postmaster@pec.lillainternational.com.

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

18 — Foro competente

Per ogni controversia relativa al presente atto è competente in via esclusiva il Foro di Latina, in conformità all'art. 31.2 delle Condizioni Generali, specificamente approvato ai sensi degli artt. 1341 e 1342 c.c.

19 — 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.

Documenti collegati: Termini e Condizioni del servizio · Informativa Privacy · Allegato Tecnico · Elenco dei sub-responsabili

Atto redatto dal Responsabile DANIELE LILLA CONSULTING (Daniele Lilla, REA LT - 315488). Versione 1.1, in vigore dal 10.08.2026: sostituisce la versione 1.0 del 15.05.2026. Tutte le versioni restano consultabili nell'archivio dei documenti legali.

Documento pubblicato da DANIELE LILLA CONSULTING · versione 1.1 · in vigore dal 10.08.2026.
Testo integrale online: crmtrasporti.com/nomina-trattamento/ — questo file: crmtrasporti.com/legal/nomina-art28-v1.1.pdf
L'impronta SHA-256 di questo file e' pubblicata nell'archivio delle versioni e non puo' essere stampata al suo interno: il calcolo comprende ogni byte del file, compresa la riga che la conterrebbe. Per verificarla: scaricare il file e confrontare il risultato di «shasum -a 256» con il valore in archivio.