

**Tirrena Sistemi S.r.l.**

Via Andrea Romaldo 8 — 84134 Salerno | P.IVA 06293660657

PEC: tirrenasistemi@postasicura.cc | info@tirrenasistemi.it

ALLEGATO C — NOMINA A RESPONSABILE DEL TRATTAMENTO

ai sensi dell'art. 28 del Regolamento (UE) 2016/679 — Servizio TShelpDesk

Contratto N. TSHD- 901_____

LE PARTI	
Titolare	Denominazione _____, sede legale in _____, P.IVA _____, C.F. _____, PEC _____, in persona del legale rappresentante (di seguito il "Titolare")
Responsabile	Tirrena Sistemi S.r.l. , sede legale in Via Andrea Romaldo 8, 84134 Salerno, P.IVA 06293660657, REA SA-512246, PEC tirrenasistemi@postasicura.cc, in persona dell'Amministratore Unico e legale rappresentante Aldo Meriano (di seguito il "Responsabile")

Premessa

Il Titolare ha stipulato con il Responsabile il Contratto di servizio TShelpDesk (il **"Contratto"**). Nell'erogare il Servizio il Responsabile tratta dati personali per conto del Titolare. Con il presente atto il Titolare **nomina** il Responsabile ai sensi dell'art. 28 del Regolamento (UE) 2016/679 ("GDPR") e il Responsabile accetta. I termini con iniziale maiuscola hanno il significato attribuito nel Contratto.

1. Oggetto, durata, natura e finalità

1.1 **Oggetto**: il trattamento dei dati personali contenuti nei Dati del Cliente, nei limiti necessari a erogare il Servizio.

1.2 **Durata**: pari a quella del Contratto, più il tempo necessario a restituire e cancellare i dati (art. 20 del Contratto e art. 10 della presente nomina).

1.3 **Natura**: raccolta e registrazione (inserimento da parte degli Utenti), organizzazione, conservazione, consultazione, elaborazione automatica secondo le funzioni del Servizio (calcolo di tempi e distanze, generazione di reportini PDF, invio di email), comunicazione al Titolare e ai suoi Utenti, cancellazione. Il Responsabile non ha accesso routinario ai contenuti: vi accede solo per assistenza, manutenzione, ripristino o sicurezza.

1.4 **Finalità**: gestione dell'attività di assistenza tecnica del Titolare (interventi, pianificazione, reportini, preventivi, richieste, parco apparecchiature, dotazione dei tecnici, portale per i clienti finali, integrazione con NTS Business se attivata).

2. Categorie di interessati e di dati

Interessati	Dati trattati
Utenti del Titolare (tecnici, amministratori, collaboratori)	nome, email, ruolo, livello tecnico; password (solo come hash); attività pianificate e svolte, tempi di lavoro, di viaggio e di rientro; coordinate GPS di partenza e di arrivo dei viaggi , rilevate dal dispositivo

Interessati	Dati trattati
	dell'Utente; tariffe e costo orario; codici di collegamento a NTS Business; note, foto, note vocali e firme caricate
Clienti finali del Titolare (persone fisiche e referenti di aziende)	nome e cognome, email, telefono, indirizzo della sede, P.IVA / C.F. (ditte individuali), ruolo; account del portale (email e password come hash); storico di interventi, preventivi, scadenze
Terzi presenti nei contenuti	firmatari dei rapportini (nome, firma grafica); mittenti di email di richiesta (nome, email, testo, allegati); voci e immagini presenti in note vocali, foto e allegati
Dati di accesso ai sistemi dei clienti finali	utenti e password delle apparecchiature, cifrati e consultabili solo previa nuova autenticazione; indirizzi IP e nomi host del parco installato

2.2 Il Titolare non inserisce nel Servizio categorie particolari di dati (art. 9 GDPR) né dati relativi a condanne penali e reati (art. 10 GDPR). Se tali dati sono inseriti nei campi liberi, ne risponde il Titolare.

3. Obblighi del Responsabile

Il Responsabile si impegna a:

- trattare i dati **solo su istruzioni documentate del Titolare**, costituite dalla presente nomina, dal Contratto e dalle funzioni del Servizio attivate dal Titolare e usate dai suoi Utenti, informando immediatamente il Titolare se ritiene che un'istruzione violi la normativa;
- garantire che le persone autorizzate al trattamento siano impegnate alla riservatezza o soggette a un obbligo legale di riservatezza e abbiano ricevuto istruzioni adeguate;
- adottare le **misure di sicurezza** dell'Allegato 2 (art. 32 GDPR);
- rispettare le condizioni dell'art. 5 per il ricorso a sub-responsabili;
- assistere il Titolare nel dare seguito alle richieste degli interessati, inoltrandogli senza ritardo quelle ricevute direttamente e astenendosi dal rispondere salvo istruzione;
- assistere il Titolare nel rispetto degli artt. 32-36 GDPR (sicurezza, notifica delle violazioni, valutazione d'impatto, consultazione preventiva) con le informazioni a sua disposizione;
- cancellare o restituire i dati alla fine del Servizio, secondo l'art. 10;
- mettere a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto dei presenti obblighi e consentire gli audit dell'art. 7;
- tenere il registro delle attività di trattamento svolte per conto del Titolare (art. 30, par. 2, GDPR);
- non trasferire i dati fuori dallo Spazio Economico Europeo (SEE).

4. Obblighi del Titolare

Il Titolare: (a) è responsabile della liceità del trattamento e della base giuridica dei dati che inserisce; (b) fornisce le informative ai propri Utenti e ai propri clienti finali — il Responsabile mette a disposizione un modello, senza assumere responsabilità sul suo contenuto; (c) valuta, con il proprio consulente del lavoro, la rilevazione della **posizione GPS dei tecnici** e le tutele sul controllo a distanza dei lavoratori (art. 4 L. 300/1970, art. 114 D.Lgs. 196/2003); (d) designa gli amministratori di sistema per quanto di sua competenza; (e) gestisce account e credenziali dei propri Utenti e decide chi accede a quali dati (ruoli "amministratore" e "tecnico"); (f) conserva i documenti che è tenuto per legge a conservare.

5. Sub-responsabili

5.1 Il Titolare **autorizza in via generale** il Responsabile a ricorrere ai sub-responsabili dell'Allegato 3, vincolati da obblighi equivalenti a quelli della presente nomina.

5.2 Il Responsabile informa il Titolare per iscritto, anche via email, di ogni aggiunta o sostituzione con preavviso di almeno **30 giorni**. Il Titolare può opporsi entro 15 giorni per motivi ragionevoli legati alla protezione dei dati; in mancanza di una soluzione condivisa, il Titolare può recedere dal Contratto senza penali per la parte di Servizio interessata.

5.3 Il Responsabile risponde verso il Titolare dell'operato dei sub-responsabili.

6. Luogo del trattamento

6.1 L'Installazione e il database sono ospitati su un'infrastruttura di proprietà del Responsabile, composta da un cluster di tre nodi in alta affidabilità, ubicato in Italia nella server farm di **Rende (CS)**, presso la quale Keliweb fornisce esclusivamente spazio fisico, alimentazione e connettività, senza accesso logico ai dati. I file (foto, firme, note vocali, allegati) e le copie di backup cifrate sono conservati sullo storage di Impossible Cloud, regione `eu-central-2`, in **Germania**. **Tutti i dati trattati dal Responsabile restano nello Spazio Economico Europeo.**

6.2 **Modulo "Assistente AI".** Il Modulo funziona esclusivamente con un account e una chiave intestati al Titolare presso il fornitore del servizio di intelligenza artificiale da lui scelto (Anthropic, PBC — Stati Uniti). Attivando il Modulo, il Titolare istruisce il Responsabile a trasmettere a tale fornitore il tipo di intervento, la descrizione dell'apparecchiatura e il testo del problema. Il fornitore del servizio opera in base al rapporto diretto con il Titolare, non è sub-responsabile del Responsabile, e il relativo trasferimento fuori dal SEE è disciplinato dal Titolare. Il Titolare può non attivare il Modulo o disattivarlo in qualsiasi momento.

7. Verifiche e audit

7.1 Il Responsabile fornisce, su richiesta, la documentazione che dimostra il rispetto degli obblighi (descrizione delle misure, esiti delle prove di ripristino, elenco dei sub-responsabili).

7.2 Il Titolare, o un revisore da lui incaricato e vincolato alla riservatezza, può svolgere un audit **una volta all'anno** e dopo una violazione dei dati, con preavviso scritto di almeno 30 giorni, in orario di lavoro, senza ostacolare l'attività e **senza accedere ai dati degli altri clienti** del Responsabile. I costi sono a carico del Titolare, salvo che l'audit riveli gravi inadempimenti del Responsabile.

8. Violazioni dei dati personali

8.1 Il Responsabile notifica al Titolare la violazione dei dati personali **entro 48 ore solari dalla conoscenza dell'evento**, in conformità con il termine di 72 ore previsto dall'art. 33 GDPR per la notifica all'Autorità Garante, all'indirizzo del referente privacy del Titolare indicato nell'Allegato A del Contratto.

8.2 La comunicazione contiene, per quanto noto: natura della violazione, categorie e numero approssimativo di interessati e di registrazioni, probabili conseguenze, misure adottate o proposte. Le informazioni mancanti sono fornite appena disponibili.

8.3 La valutazione del rischio, la notifica al Garante e la comunicazione agli interessati competono al Titolare. Il Responsabile collabora fornendo le informazioni tecniche disponibili e adotta le misure per contenere la violazione e prevenirne il ripetersi.

9. Misure di sicurezza

Le misure sono descritte nell'Allegato 2. Il Responsabile può aggiornarle nel tempo purché non riduca il livello di protezione.

10. Restituzione e cancellazione

10.1 Alla cessazione del Contratto il Responsabile, a scelta del Titolare comunicata per iscritto, **restituisce** i dati (esportazione e file) o li **cancella**, nei tempi dell'art. 20 del Contratto. La cancellazione comprende database, file, chiavi e backup (backup locali entro 14 giorni, copie esterne entro 30 giorni).

10.2 Il Responsabile rilascia, su richiesta, attestazione scritta dell'avvenuta cancellazione.

10.3 Il Responsabile può conservare i dati solo se un obbligo di legge lo impone, informandone il Titolare.

11. Responsabilità

11.1 Ciascuna Parte risponde verso gli interessati ai sensi dell'art. 82 GDPR, norma inderogabile.

11.2 Nei rapporti tra le Parti, per i danni derivanti dalla violazione, dovuta a colpa lieve del Responsabile, degli obblighi della presente nomina o del GDPR, la responsabilità complessiva del Responsabile è limitata a un importo pari al **doppio dei canoni corrisposti dal Titolare nei 12 mesi precedenti** il fatto o, nel primo anno, al doppio del canone annuo previsto. Tale limite sostituisce, per questi danni, quello dell'art. 21.2 del Contratto e non si cumula con esso.

11.3 Restano ferme l'esclusione per colpa lieve quando la mancata collaborazione del Titolare sia stata causa determinante del danno (art. 21.3 del Contratto) e l'esclusione dei danni indiretti (art. 21.4 del Contratto). Nessun limite si applica in caso di dolo o colpa grave (art. 1229 c.c.).

12. Contatti

REFERENTI PER LA PROTEZIONE DEI DATI	
Referente privacy del Titolare	Nome: _____, email: _____, telefono: _____
Referente privacy del Responsabile	dpo@tirrenasistemi.it — tel. 089 8424641

Il Responsabile non ha nominato un Responsabile della protezione dei dati (DPO), non essendo obbligatorio; i riferimenti sopra valgono per ogni comunicazione.

Luogo e data: _____

Il Titolare — il legale rappresentante

Il Responsabile — Tirrena Sistemi S.r.l.

Data: ____ / ____ / ____

Data: ____ / ____ / ____

Allegato 1 — Categorie di trattamento

Si rinvia agli artt. 1.3 e 1.4 (natura e finalità) e all'art. 2 (interessati e dati) della presente nomina.

Allegato 2 — Misure tecniche e organizzative di sicurezza

Misure in funzione alla data di sottoscrizione. Ogni modifica che incida sulle misure comporta l'aggiornamento del presente allegato.

Controllo degli accessi

- Accesso con email e password e **seconda verifica obbligatoria** con codice monouso inviato per email a ogni accesso, valido 10 minuti, con massimo 5 tentativi.
- Password conservate solo come **hash bcrypt**, mai in chiaro; lunghezza minima 8 caratteri.
- Limiti ai tentativi di accesso, di verifica del codice e di recupero password, per indirizzo e per account, con protezione contro tentativi distribuiti.
- Ruoli distinti (amministratore, tecnico); le operazioni di amministrazione sono riservate agli amministratori.
- Un utente disattivato perde immediatamente l'accesso; il ruolo effettivo è sempre quello attuale in archivio.
- Sessioni con scadenza (8 ore per lo staff); nelle licenze a sessioni limitate il collegamento si chiude al logout.
- File caricati accessibili **solo con sessione valida**, tramite cookie riservato non leggibile da script e non inviato da altri siti.
- Credenziali delle apparecchiature conservate **cifrate (AES-256-GCM)** e mostrate solo dopo il reinserimento della password personale, con limite ai tentativi e registrazione della consultazione.
- Portale clienti con account separati dallo staff, accesso su invito; ogni cliente finale vede esclusivamente i propri dati.

Separazione tra clienti

- Ogni cliente ha **database, spazio file, chiavi di cifratura e codice di attivazione propri**; il servizio di ciascun cliente gira come processo separato.

Protezione dei dati in transito e a riposo

- Comunicazioni in **HTTPS** con certificato gestito dal Responsabile per tutti i sottodomini *.help24ore.it; intestazioni di sicurezza attive.
- Chiavi e segreti di terzi (es. chiave del servizio AI del Titolare, password della casella email, chiavi di backup delle apparecchiature) cifrati nel database.
- Copie di backup esterne cifrate prima dell'invio allo storage: il fornitore dello storage non può leggerle.

Disponibilità e ripristino

- **Backup del database ogni notte**, verificato prima di essere accettato e conservato 14 giorni sull'Infrastruttura.
- **Copia esterna cifrata** (AES-256 con derivazione della chiave) su archivio e account separati, riletta e confrontata, conservata 30 giorni; controllo giornaliero con avviso per email in caso di mancata esecuzione.
- **Prova di ripristino** documentata, di norma ogni mese.
- Infrastruttura in cluster a tre nodi in alta affidabilità; riavvio automatico del servizio in caso di arresto; limiti di tempo alle richieste e ai collegamenti verso servizi esterni.
- **Monitoraggio automatico** ogni 5 minuti di servizi, database, raggiungibilità dell'indirizzo pubblico, certificati, backup, licenze e spazio disco, con avviso per email.

Gestione delle modifiche

- Aggiornamenti tramite procedura che esegue un **backup preventivo**, verifica il funzionamento e **ripristina la versione precedente** in caso di problemi.
- Codice sottoposto a controlli di tipo e di compilazione; dipendenze aggiornate con le correzioni di sicurezza disponibili; prove di attacco interne su ambiente isolato (accessi, token, isolamento tra clienti, carico, interruzione del database).

Misure organizzative

- Accesso privilegiato all'Infrastruttura riservato alle sole persone dell'Allegato 4, individuate nominativamente quali amministratori di sistema.
- **Registri degli accessi** degli amministratori di sistema attivi sull'Infrastruttura e conservati per almeno sei mesi (Provvedimento del Garante del 27 novembre 2008).
- Procedura scritta di gestione delle violazioni dei dati personali.
- Ogni nuova persona autorizzata riceve autorizzazione scritta, sottoscrive un impegno di riservatezza e riceve formazione sulla protezione dei dati prima di accedere ai dati.

Limiti dichiarati

- Il Servizio non dispone, alla data di sottoscrizione, di certificazioni (es. ISO/IEC 27001) né di verifiche di sicurezza svolte da un soggetto terzo indipendente.
- Non è attivo un servizio di reperibilità 24 ore su 24: gli avvisi sono gestiti negli orari di assistenza; l'obiettivo di disponibilità dell'Allegato B è un obiettivo, non una garanzia.

Allegato 3 — Sub-responsabili autorizzati

Sub-responsabile	Servizio	Dati	Localizzazione
Impossible Cloud GmbH	storage dei file del Servizio (foto, firme, note vocali, allegati) e delle copie esterne cifrate dei backup	file del Servizio; copie di backup cifrate, non leggibili dal fornitore	regione eu-central-2 — Germania (SEE)

Non sono sub-responsabili: Keliweb, che fornisce al Responsabile solo spazio fisico, alimentazione e connettività nella server farm di Rende (housing), senza accesso logico ai dati; il server di posta del Servizio, gestito direttamente dal Responsabile (mail.tirrenasistemi.net); NTS Business, servizio del Titolare; il fornitore del servizio di intelligenza artificiale, con cui il Titolare ha un rapporto diretto (art. 6.2).

Allegato 4 — Persone autorizzate del Responsabile

Nome	Ruolo	Accesso	Riservatezza
Aldo Meriano	Amministratore Unico e legale rappresentante; amministratore di sistema dell'Infrastruttura	server, database, backup, storage, Installazioni dei clienti	obbligato in quanto legale rappresentante del Responsabile

Alla data di sottoscrizione non vi è altro personale con accesso ai dati. L'eventuale ingresso di nuove persone autorizzate è comunicato al Titolare su richiesta.